

CONFIGURATION MIGRATION TOOL

FortiConverter User Guide

VERSION 4.8

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



Monday, October 19, 2015

FortiConverter 4.8 User Guide

1st Edition

TABLE OF CONTENTS

Introduction	6
SFTP service for submitting configuration files	6
Supported vendors & configuration objects	7
Licensing	9
System requirements	9
What's new	10
Installing the software	12
Uploading the license	13
Conversion	17
Downloading the source configuration files	17
Alcatel-Lucent	17
Check Point	18
Cisco	19
Fortinet	19
Juniper	19
Palo Alto Networks	20
SonicWall	20
Using the conversion wizards	20
Alcatel-Lucent conversion wizard	21
Start Options	21
Source Configuration Selection	22
Device Selection	23
Partition & Zone Rule Selection	24
Physical Interface Mapping	25
VLAN and Loopback	26
Route Information	27
Conversion Result	28
Check Point conversion wizard	28
Including object comments in the output configuration	28
Start Options	29
Start Options - More	30
MDS Source Configuration (Provider-1 only)	32
MDS Selection (Provider-1 only)	33
Global Policy Collection Selection (Provider-1)	34

Domain Source Configuration	35
Policy Collection Selection	36
Firewall Selection (SmartCenter only)	37
Physical Interface Mapping (SmartCenter only)	38
Route Information (SmartCenter only)	39
Conversion Result	40
Cisco conversion wizard	41
Start Options	41
Source Configuration Selection	42
Context Selection	43
Physical Interface Mapping	44
VLAN and Loopback	45
Route Information	46
VPN Phase2	47
Conversion Result	48
Fortinet conversion wizard	49
Start Options	49
Source Configuration Selection	50
VDOM Selection	51
Physical Interface Mapping	52
Additional Rule	53
Conversion Result	54
Juniper conversion wizard	55
Start Options	55
Source Configuration Selection	56
LSYS (Junos OS) or VSYS (ScreenOS) Selection	57
Physical Interface Mapping	58
Route Information	59
Conversion Result	60
Palo Alto conversion wizard	61
Start Options	61
Source Configuration Selection	62
VSYS Selection	63
Physical Interface Mapping	64
Conversion Result	65
SonicWall conversion wizard	65
Start Options	66
Source Configuration Selection	67
Physical Interface Mapping	68
VLAN and Loopback	69
Route Information	70
Conversion Result	71

Snort conversion wizard	72
Start Options	72
Rule Variables	73
Conversion Result	74
Using retail branch batch conversion mode	74
Batch mode for Cisco, Juniper, Palo Alto Networks, and SonicWall firewalls	75
Batch mode for Alcatel-Lucent and Check Point firewalls	76
Viewing the results of your automatic conversion	79
Tuning the FortiConverter output	81
Toolbar options	81
Policy Tuning tab	82
NAT Merge Review tab	86
Conversion log tab	89
Importing your new configuration into FortiManager	91
Output from conversion to FortiManager	91
Import your new configuration into FortiManager	92
Understanding your new configuration	96
Alcatel-Lucent differences	96
Conversion support	96
Address and address group configuration	96
Interface configuration	96
Service and Service Group configuration	96
Policy configuration	96
VDOM configuration	98
Example conversion	98
Check Point differences	100
General	100
Schedule configuration	100
NAT and policy configuration	100
VPN configuration	101
Service objects	101
Cisco IOS, PIX or ASA differences	101
Juniper ScreenOS or Junos OS differences	102
Palo Alto Networks OS (PAN-OS) differences	102
Conversion support	102
Configuration notes	103

Introduction

This document shows how to install and use FortiConverter.

FortiConverter is designed to help you migrate your network to Fortinet network security solutions, significantly reducing workload and minimizing errors. FortiConverter translates configuration files from other vendors' firewall products into a valid FortiGate or FortiManager configuration file. Because the output uses command line syntax, it can either be uploaded as a configuration file or piped to the CLI.

For additional assistance, please contact fconvert_feedback@fortinet.com.

SFTP service for submitting configuration files

FortiConverter customers can securely submit firewall configuration files to Fortinet Engineering using Fortinet's SFTP service.

Because this account has many restrictions, Fortinet recommends that you use a command-line SFTP client to transfer files. For example, [Cygwin](#) provides a suitable SFTP client for Windows users.

To upload a file

1. Connect to the SFTP using the following settings:

Server	ftp.apsecure.com
Port	2222
User	fcon-incoming
Password	incoming

2. Create a folder using your FortiConverter serial number for its name.
3. Post your files in the new folder.

Example connection

```
sftp -P 2222 fcon-incoming@ftp.apsecure.com
$ sftp -P 2222 fcon-incoming@ftp.apsecure.com
fcon-incoming@ftp.apsecure.com's password:
Connected to ftp.apsecure.com.
sftp> ls
remote readdir("/home/fcon/incoming"): Permission denied
sftp> mkdir FCON010000010864
sftp> cd FCON010000010864
sftp> pwd
Remote working directory: /home/fcon/incoming/FCON010000010864
sftp> put config.rar
Uploading config.rar to /home/fcon/incoming/FCON010000010864/config.rar
config.rar 100% 3826KB 273.3KB/s 00:14
sftp> ls
```

```
config.rar
sftp> bye
```

Supported vendors & configuration objects

FortiConverter can translate configurations from the following vendors and platforms.

In some cases, FortiConverter cannot translate some parts of the configuration because of dependencies or unsupported syntax and you must manually convert them.

If the number of objects exceeds the maximum valid length for FortiGate or FortiManager, FortiConverter trims them.

Vendor	Models	Versions	Convertible objects
Alcatel-Lucent	Brick	v9.x	Addresses & Address Books Interfaces (physical, logical, loopback, PPPoE) Partitions Services & Service Books Static routes Zone rule set
Check Point	SmartCenter Provider-1	NG FP1 (4.) to NGX R64/R71/R75/R76	Addresses & Address Groups Interfaces (Physical, Logical, Loopback, PPPoE) Local Users & Groups NAT (Automatic & Rule) Negate Cell Policies (rulebases.fws) RADIUS, TACACS+, & LDAP Rules Schedules Services & Service Groups Static routes VPN (IPSec)
Cisco	PIX ASA FWSM	4.x to 8.x	ACLs Addresses & Address Groups DHCP Servers DNS Servers Interfaces (Physical, Logical, Loopback, PPPoE, Tunnel) IP Pools Local Users & Groups NAT (including Object NAT and Double NAT) RADIUS, TACACS+, & LDAP Services & Service Groups Static Routes Time Ranges VPN (IPSec, PPTP/L2TP, EZVPN)
	IOS	10.x to 12.x 15.x	

Vendor	Models	Versions	Convertible objects
Juniper	SSG	ScreenOS/Junos OS 5.x to 6.x	Addresses & Address Groups & FQDNs DHCP Servers & Clients & Relays Interfaces (Physical, Logical, Loopback, PPPoE, Tunnel) Static Routes Services & Service Groups Policies VIPs/MIPs NAT IP Pools VPN (IPSec, PPTP/L2TP) Local Users & Groups RADIUS & LDAP Zones
	SRX	Junos OS 10.x, 11.x, 12.x	Addresses & Address Groups & FQDNs DHCP Servers & Client & Relay Interfaces (Physical, Logical, Loopback, PPPoE, Tunnel) IP Pools Local Users & Groups NAT Policies RADIUS & LDAP Services & Service Groups Static Routes VIPs/MIPs VPN (IPSec, PPTP/L2TP) Zones
Palo Alto Networks	PA	PAN-OS 1.x to 6.x	Addresses & Address Groups & FQDNs Interfaces Local Users & Groups NAT (partial) Policies Schedules Static Routes Services & Service Groups Zones
SonicWall	NSA Serials	SonicOS Enhanced 5.x	Addresses & Address Groups & FQDNs DHCP Servers & Clients & Relays Interfaces (Physical, Logical, Loopback, PPPoE) Local Users & Groups NAT Policies Schedules Services & Service Groups Static Routes Zones

Licensing

The trial version of FortiConverter provides full conversion functionality for FortiGate-to-FortiGate conversions. It supports trial conversions for Cisco, Check Point, and Juniper. Trial conversions allow you to review of conversion results and generate 100 lines of configuration output, but the fine-tuning features are disabled.

The trial version does not support Alcatel-Lucent, Snort, Sonicwall, and Palo Alto Network conversions.

After you purchase and upload a license, FortiConverter is unlocked and full conversion functionality is enabled for all supported vendors. Your paid license entitles you to any new versions of FortiConverter that Fortinet releases until the license expires.

FortiConverter requires an Internet connection to verify its license. You can use the software for up to 30 days without validating the license online.

For more information, see ["Uploading the license" on page 13](#)

System requirements

FortiConverter requires one of the following operating systems:

- Microsoft Windows 10
- Microsoft Windows 8 (32-bit or 64-bit)
- Microsoft Windows 7 (32-bit or 64-bit)
- Microsoft Windows Server 2008 (32-bit or 64-bit)

In addition, FortiConverter requires .NET Framework 4.0. If it is not already installed on your computer, the FortiConverter installer prompts you to download and install it.

A web browser is required to view conversion reports.

An Internet connection is required to verify the software license.

What's new

The following list contains features that are new or enhanced since FortiConverter 4.4.

FortiConverter 4.8

- **Check Point conversion**
 - **Comment fields** – New options allow you to convert Check Point interface, address, service, and rule comments.
 - **Review memo** – You can now export NAT merge converted policies as a separate file for review purposes.
 - **NAT conversion** – FortiConverter now supports the conversion of both manual and automatic NAT rules and both static and hide NAT types.
 - **NAT merge review** – The tuning features for Check Point conversions now include a NAT Merge Review tab. Use it to review how FortiConverter merged NAT and firewall policies to create corresponding FortiOS policies.
 - **Service protocol type** – FortiConverter now supports the conversion of Check Point service object definitions that include a protocol type by using a FortiOS session helper.
- **Cisco conversion**
 - **Virtual contexts** – Virtual contexts are now supported. You can select individual virtual contexts to convert to equivalent VDOMs.
 - **PIX conversion** – FortiConverter now supports the conversion of Static, Policy, and Dynamic NAT and Port Address Translation (PAT) for PIX configurations.
- **Fortinet conversion**
 - **New conversion targets** – You can now select FortiOS v5.0 or v5.2 as the target for FortiGate-to-FortiGate conversions.
 - **Restorable configuration** – A new option allows you to generate configuration files that can be directly restored to the target device.
- **Juniper conversion**
 - **Enhanced conversion logic for ScreenOS** – FortiConverter now supports conversion of additional configuration objects, including redundant and VLAN1 interfaces and HA configuration.
 - **MS-RPS and SUN-RPC conversion for JunOS** – FortiConverter now supports the conversion of MS-RPS and SUN-RPS firewall services.
- **Reload exported result** – Use the Tuning button on any wizard page to load any conversion result that you exported earlier.
- **Context-sensitive help** – Click the Help button to display online help information for the current FortiConverter page in your web browser.

FortiConverter 4.7

- **Junos OS NAT merge review** — FortiConverter can now perform a NAT merge between security rules and NAT tables based on address comparison. The NAT tuning page now provides details about the conversion logic for FortiGate NAT policies. See [NAT Merge Review tab on page 86](#)
- **FortiOS 4.x to 5.x conversion** — FortiConverter now supports a limited conversion from FortiOS 4.x to FortiOS 5.x. See [Fortinet conversion wizard on page 49](#).

- **Junos OS Logical System (LSYS) and ScreenOS Virtual System (VSYS)** — FortiConverter converts LSYS and VSYS to FortiGate VDOMs. See [Juniper conversion wizard on page 55](#).
- **Save Fortinet conversions using the trial version** — You do not need to upload a paid license for FortiConverter before you can save your Fortinet-to-Fortinet conversions.
- **Results page web UI enhancements** — The wizard's Conversion Result page is now grouped into categories for quick review. An Export button allows you to save conversion statistics as an HTML page. For more information, see the wizard information for the vendor you want to convert.
- **Policy review wizard page** — This additional page displays detailed address/service object list information. See [Policy Tuning tab on page 82](#).
- **Import instructions** — The conversion headers of FortiConverter output files now provide instructions for building the new configuration file. For FortiGate-to-FortiGate conversions, you simply restore the outputs, and for Snort conversions, you import the outputs.

FortiConverter 4.6

- **FortiGate to FortiGate conversion** — Move a configuration to one or more FortiGate devices using either Migrate or Split VDOMs mode. See [Fortinet conversion wizard on page 49](#).
- **Partition and zone selection in Lucent Brick conversions** — You can select or deselect individual partitions and zones when you convert.
- **Generate NAT rules and mappings from Hide NATs in Check Point conversions** — Use Hide NATs to create the NAT rules and mappings that are specified by the `central-nat` CLI commands in FortiGate. To use, select **Enable Central NAT merge** on the Start Options page.
- **Auto-generate interface policies using the route table in Check Point conversions** — To use, select **Auto generate policy interfaces** on the Start Options page, and then add a route file on the Firewall Selection page.
- **Export or import interface maps** — You can now save and restore interface assignments.
- **Export or import tuning snapshots** — You can now save post-conversion tuning changes.

FortiConverter 4.5

- **Palo Alto Networks firewall conversion** — FortiConverter can now convert a Palo Alto Networks firewall configuration to a FortiOS configuration. See ["Supported vendors & configuration objects" on page 7](#).
- **Batch mode for retail branch conversion** — You can now convert a group of firewalls using a single operation. See ["Using retail branch batch conversion mode" on page 74](#).
- **Automatically check for updates** — You can configure FortiConverter to automatically check for software updates.
- **Configurable policy index values** — You can now select the initial policy number that FortiConverter uses in a converted configuration. See ["Tuning the FortiConverter output" on page 81](#).
- **Output file directory** — FortiConverter now saves converted configurations as files in a directory with the name of the input file. If subsequent input files have a different name, it preserves any previous output files.

Installing the software

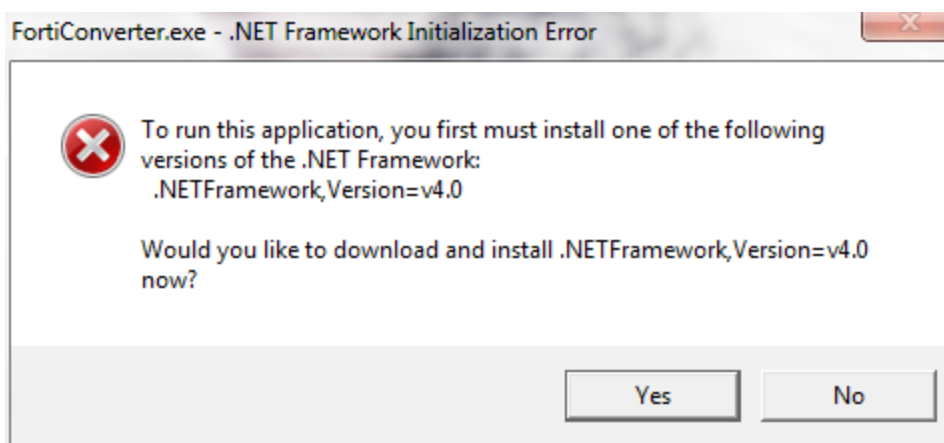
To download the FortiConverter installer from the Fortinet Technical Support web site, go to:

<https://support.fortinet.com>

To install FortiConverter

1. Double-click the FortiConverter installer executable (.exe).

If your computer does not have Microsoft .NET Framework 4.0, you are prompted to install it.



2. To proceed with the installation, click **Yes** and then download the software framework from Microsoft's web site.
3. To continue the installation, read the license agreement, select **I accept the terms of the License Agreement**, and then click **Next**.
4. If you want to install the program in a location that is different from the default one, click **Browse** and select the directory.
5. Click **Next**.
6. Select the Start Menu folder that you want to add the program shortcuts to, and then click **Install**.
7. Click **Finish** to exit the FortiConverter installer.

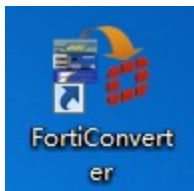
Uploading the license

By default, FortiConverter is installed with a limited, trial license. If you have purchased an full license, upload it to unlock the complete feature set.

To purchase a license, use your usual Fortinet sales channel.

To activate the license

1. To start FortiConverter, double-click its shortcut.

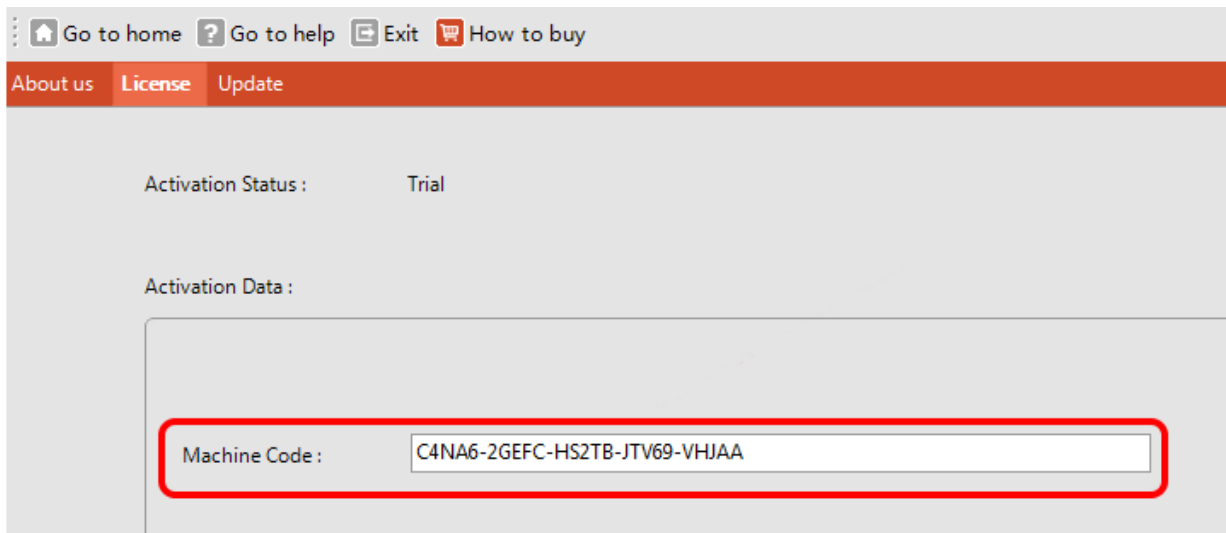


2. Click **About FortiConverter**.



3. Click the **License** tab.

4. Copy the **Machine Code** value to the clipboard.



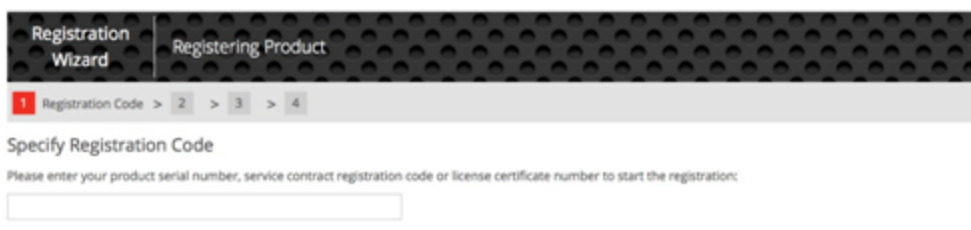
5. Ensure you have purchased a license, and then sign in to the Fortinet Technical Support web site at the following location:

<https://support.fortinet.com/>

Registration uses a simple, four-step wizard that is common to many Fortinet products.

6. On the first page of the wizard, for the registration code, enter the SKU for your FortiConverter product.

The FortiConverter release notes provide the SKUs (go to docs.fortinet.com/forticonverter).



7. For step 2 of the registration wizard, for **Hardware ID**, enter the **Machine Code** value you copied earlier.

The screenshot shows the 'Contract Registration' wizard for 'Registering FortiConverter'. The progress bar indicates Step 2 'Registration Info' is active. The page title is 'Specify Fortinet Registration Information'. Below the title, there are three sections with input fields: 'Please specify your hardware id' with a 'Hardware ID:' field; 'To help you identify this product, you may enter a description here' with a 'Product Description:' field; and 'Please specify your Fortinet Partner or Reseller helped you with this product' with a 'Fortinet Partner:' dropdown menu. A 'Contract Number' is displayed in the top right corner.

8. After you agree to the license terms, the final page of the wizard (step 5) allows you to download the license file (.lic file).

The screenshot shows the 'Contract Registration' wizard for 'Registering FortiConverter'. The progress bar indicates Step 5 'Completion' is active. The page title is 'Registration Completed'. Below the title, there is a message: 'Thank you for choosing Fortinet product. Your registration process has successfully completed. Please be aware that the registration information may not reflect on your product immediately, a delay (up to 4 hours) can occur.' Below this message, there is a 'Product Info' section with a 'General' tab. The 'General' tab displays the following information: Product Model: FortiConverter, Serial Number: FCON010000010135, Registration Date: 2014-01-24, Description: N/A, Partner: Fortinet, and License File: [License File Download](#). A 'Contract Number' is displayed in the top right corner.

9. In FortiConverter, on the License tab, click **Select** and navigate to the .lic file to select it.
10. Click **Activate**.

FortiConverter validates the license file and changes the value of **Activation Status** from **Free** to **Activated**.

The screenshot shows the 'License' tab in the FortiConverter application. At the top, there are three tabs: 'About us', 'License' (which is selected and highlighted in orange), and 'Update'. Below the tabs, the 'Activation Status' is 'Activated' and the 'License Expire Date' is '2017-01-07'. These two items are enclosed in a red rectangular box. Below this, the 'Activation Data' section contains a 'Machine Code' field with the value 'C4NA6-2GEFC-HS2TB-JTV69-VHJAA' and a 'License File' field with the value 'C:\Downloads\License.lic'. To the right of the 'License File' field is a 'Select' button. At the bottom right of the 'Activation Data' section is an 'Activate' button.

Activation Status	
Activation Status :	Activated
License Expire Date:	2017-01-07

Activation Data :

Machine Code :	C4NA6-2GEFC-HS2TB-JTV69-VHJAA
License File :	C:\Downloads\License.lic

Select

Activate

Your license is valid for all FortiConverter software updates released until the **Expire Date** value.

After the license is activated, to access the expiry information, on the home page, click **System Setting**, and then click the **License** tab.

Conversion

FortiConverter provides wizards that convert configuration files from a specific vendor to FortiGate or FortiManager configuration files. After you input information about your previous vendor's configuration files, you can preview and fine-tune the conversion before you output the final FortiGate or FortiManager configuration file.

Downloading the source configuration files

Before you start the conversion wizard, download your existing configuration to the computer where FortiConverter is installed. Procedures vary by vendor.

Some vendors divide the configuration into multiple files, so make sure that you download all files.

Alcatel-Lucent

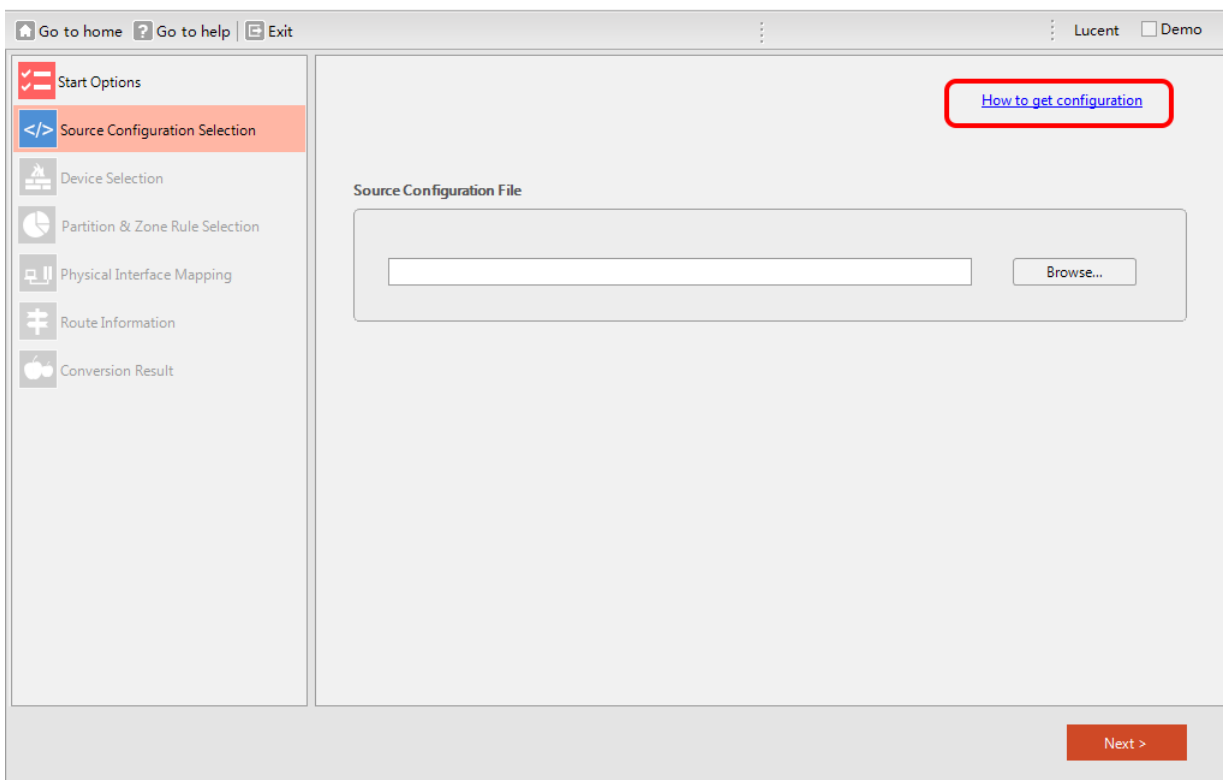
FortiConverter provides a Perl script for downloading Alcatel-Lucent Brick configurations.

To access the Alcatel-Lucent configuration download script

1. On the FortiConverter home page, click the Alcatel-Lucent square.
2. On the Start Options page, click **Next**.

If you are using the wizard to retrieve the download script only, use the default settings for this page. You can restart the wizard later after you have the file and are ready to perform the conversion with the appropriate settings.

3. On the Source Configuration Selection page, click **How to get configuration**.



The Windows folder that contains the Perl script and the documentation for using it are displayed. Follow the instructions to run the Perl script and output the source configuration as a set of directories.

Check Point

To acquire the configuration, download the following files. In most cases, you download the object and policy definitions from the management system:

- Object definitions — 'objects_5_0.C' (Check Point NG/NGX) or 'objects.C' (Check Point 4.x) contain the firewall's object definitions. To convert from Provider-1, 'mcsc.C' contains the MDS hierarchy files.
- Policy and rule definitions — '*.w' or 'rulebases_5_0.fws'. The file name is <rule>.W (default Standard.W). or rulebases_5_0.fws. They are located in the directory "[SmartCenter] : \$FWDIR/conf".
- Route information (optional) — Helps FortiConverter to correctly interpret the network topology being converted. To get this data, enter the `route print` command on the firewall node, and then copy and paste the output into a plain text file. Codes in the output indicate if the route is a directly connected interface, a host route, a network route, and so on. The output varies by the platform.
- User and user groups file (optional) — fwauth.NDBx

File	File name	Path
Object definitions	objects_5_0.C (Checkpoint NG/NGX)	\$FWDIR/conf
	objects.C (Checkpoint 4.x_)	

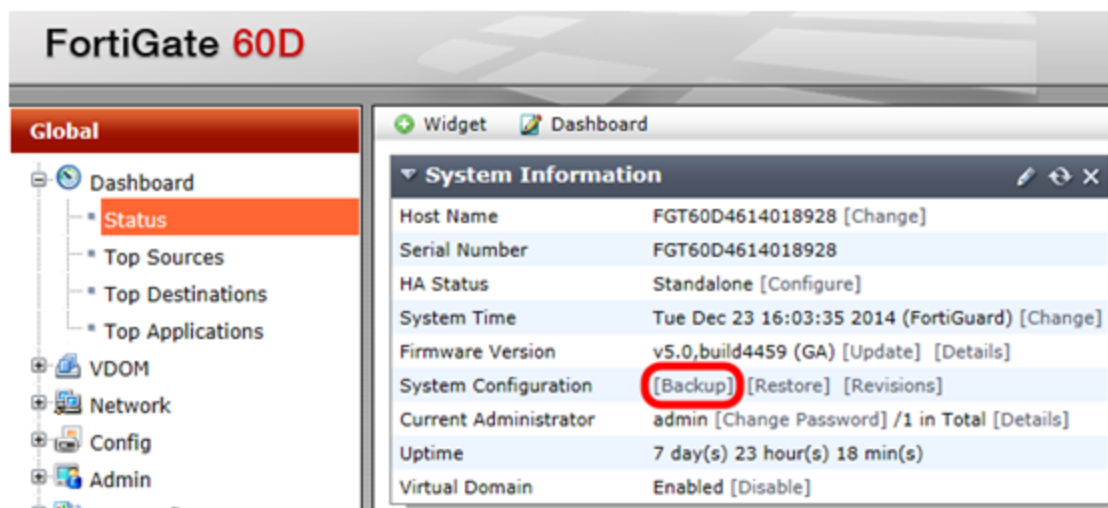
File	File name	Path
	mcss.C (Provider-1)	\$MDSDIR/conf/mdsdb
Policy and Rule definitions	rulebase_5_0.fws [package name].W	\$FWDIR/conf
Route information	NA	Save output of route print command from firewall
User and User Group file	fwauth.NDBx	\$FWDIR/conf/ or \$FWDIR/database/

Cisco

To acquire the configuration, enter the `show running-config` command, and then paste the output into a plain text file.

Fortinet

Go to **Configuration > Update > ConfigFile**. Use the web UI to download the configuration.



Juniper

To obtain the configuration, use one of the following methods:

- In the web UI, go to **Configuration > Update > ConfigFile**.
- Using the CLI, paste the output of the `get conf` command into a plain text file.

Palo Alto Networks

In the web UI, go to **Device > Setup > Operations**, and then click **Export named configuration snapshot**.

SonicWall

To download the configuration (*.exp file), in the web UI, go to **System > Settings > Export Settings**.

Using the conversion wizards

To access the conversion wizards, from the main FortiConverter window, click the appropriate icon.

FortiConverter has a separate wizard for each supported vendor. The settings for each wizard type are described in the sections that follow this introduction.

Each wizard has a demo configuration file that can be selected using the Demo check box in the upper right corner.

The settings that are displayed depend the input configuration. For some conversions, not every page in the wizard is displayed.

Alcatel-Lucent conversion wizard

Start Options

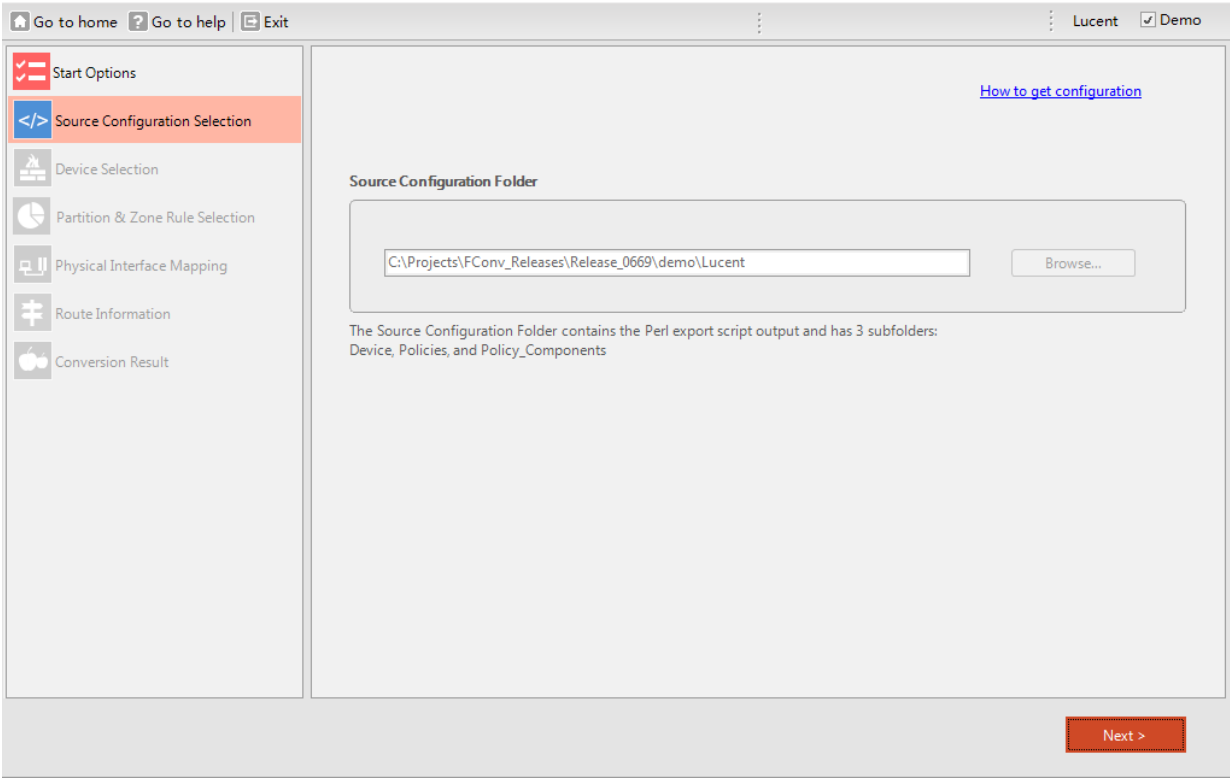
The screenshot shows the 'Start Options' window of the Alcatel-Lucent conversion wizard. The window has a sidebar on the left with a 'Start Options' button. The main area contains the following settings:

- Model:** A dropdown menu with 'LucentBrick' selected.
- Output Format:** A dropdown menu with 'FortiGate' selected.
- Output OS Version:** Two radio buttons, 'v 4.x' and 'v5.x', with 'v5.x' selected.
- Conversion Option:** Two checkboxes, 'Discard unreferenced firewall objects' and 'Set policy comment with source config line', both of which are checked.
- Output Directory:** A text input field containing 'C:\FortiConverterOutput' and a 'Browse...' button.

A 'Next >' button is located at the bottom right of the window.

Setting	Description
Model	LucentBrick is the only supported model.
Output Format	FortiGate is the only supported output format.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Set policy comment with source config line	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Output Directory	Select the folder where the output configuration is saved.

Source Configuration Selection



Setting	Description
Source Configuration Folder	Select the input folder.

Device Selection

Go to home ? Go to help Exit

Lucent ☒ Demo

☒ Start Options

☐ Source Configuration Selection

☒ Device Selection

☐ Partition & Zone Rule Selection

☐ Physical Interface Mapping

☐ Route Information

☐ Conversion Result

Please select the firewall which you want to convert:

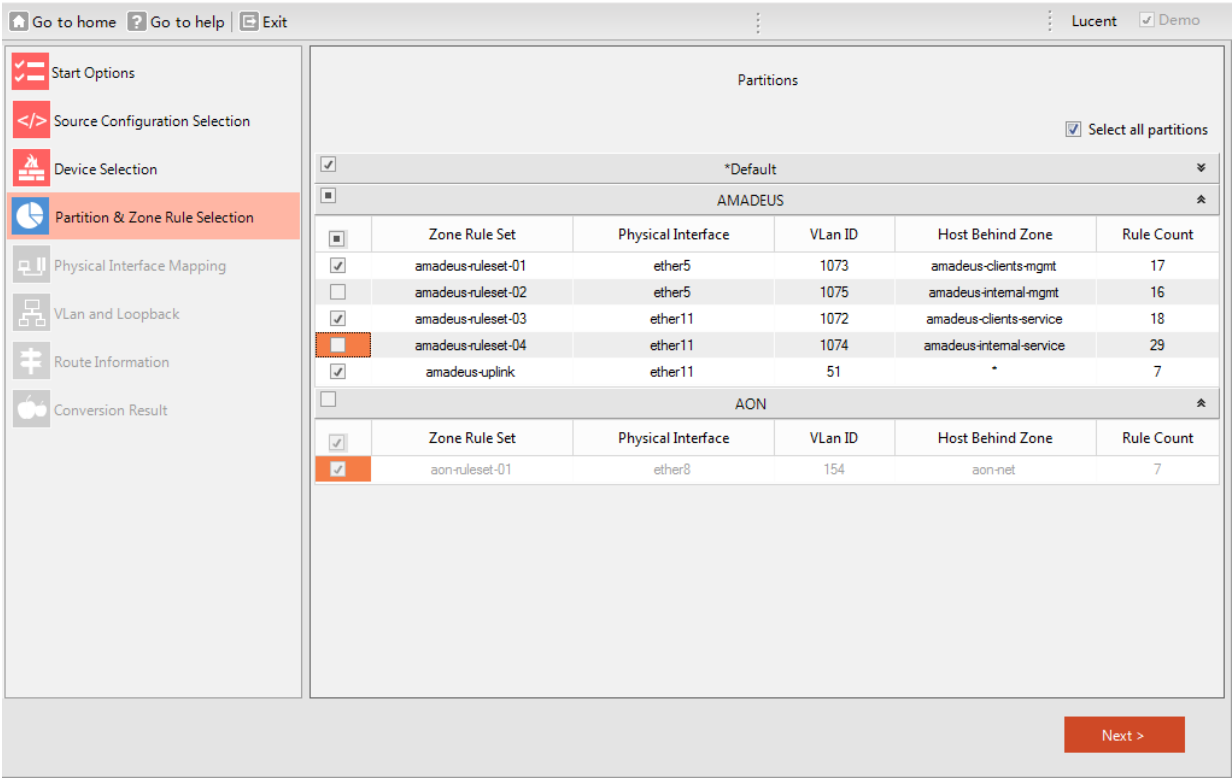
☒ lucent-demo-test01

☐ Retail Branch Batch Mode

Next >

Setting	Description
Retail Branch Batch Mode	Select to specify multiple firewalls from the list. Select only firewalls with the same interfaces. For more information, see Using retail branch batch conversion mode on page 74
Device Selection	Select the firewalls to convert.

Partition & Zone Rule Selection



Setting	Description
Select all partitions	Select to select all partitions and clear it to de-select all partitions. Use the check box to select a partition to include in the conversion.
Partition selection	Click the pair of arrows on the right to open or close the detailed partition view, which shows the individual zone rules within a partition.
Zone rule selection	Use the check box to select a zone rule to include in the conversion.

Physical Interface Mapping

Go to home ? Go to help Exit Lucent Demo

- Start Options
- Source Configuration Selection
- Device Selection
- Partition & Zone Rule Selection
- Physical Interface Mapping**
- Vlan and Loopback
- Route Information
- Conversion Result

Physical Interface Mapping
Please click the '?'

Name	IP	Netmask	Alias	Status	FG Port
*Default					
ether0	66.119.71.49	255.255.255.240	VLAN 26	up	port1
ether1			VLAN 98	up	port2
ether2	66.119.71.49	255.255.255.240	VLAN 26	up	?
ether3			VLAN 1	up	?
ether4			VLAN 478	up	?
ether5			VLAN 95	up	?
ether6			VLAN 98	up	?
ether7			VLAN 1	up	?
ether8			VLAN 98	up	?
ether9			VLAN 98	up	?
ether10			VLAN 98	up	?
ether11			VLAN 96	up	?
ether12	10.194.96.5	255.255.255.248	VLAN 127	up	?
ether13	172.21.225.225	255.255.255.240	VLAN 100	up	?
ether14			VLAN 631	up	?
ether15	172.21.225.225	255.255.255.240	VLAN 100	up	?
ether16	172.21.225.225	255.255.255.240	VLAN 100	up	?

Import Export

Next >

Setting	Description
FG port	Click to assign a FortiGate port for each interface.
(table column)	Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

VLAN and Loopback

Go to home
Go to help
Exit
Lucent
☒ Demo

Start Options

Source Configuration Selection

Device Selection

Partition & Zone Rule Selection

Physical Interface Mapping

Vlan and Loopback

Route Information

Conversion Result

VLAN and Loopback Interface

Name	IP	Netmask	Alias	Status
*Default				
VLAN26	66.119.71.49	255.255.255.240		up
VLAN74	10.255.252.70	255.255.255.248		up
VLAN75	10.255.252.78	255.255.255.248		up
VLAN464	10.255.24.1	255.255.255.192		up
VLAN465	10.255.24.65	255.255.255.192		up
VLAN466	10.255.25.1	255.255.255.0		up
VLAN468	10.255.24.129	255.255.255.192		up
VLAN181	192.168.181.69	255.255.255.252		up
VLAN219	192.168.35.1	255.255.255.224		up
VLAN220	192.168.35.33	255.255.255.224		up
VLAN222	192.168.35.193	255.255.255.224		up
VLAN223	192.168.35.97	255.255.255.224		up
VLAN224	192.168.35.129	255.255.255.240		up
VLAN225	192.168.35.145	255.255.255.240		up
VLAN226	192.168.35.161	255.255.255.240		up
VLAN230	192.168.24.161	255.255.255.240		up
VLAN231	192.168.24.177	255.255.255.240		up
VLAN235	192.168.24.193	255.255.255.240		up
VLAN236	192.168.24.209	255.255.255.240		up
VLAN239	192.168.24.225	255.255.255.240		up

Next >

For information only. No settings.

Route Information

Go to home
Go to help
Exit
Lucent
Demo

Start Options
Source Configuration Selection
Device Selection
Partition & Zone Rule Selection
Physical Interface Mapping
VLAN and Loopback
Route Information
Conversion Result

Route Information

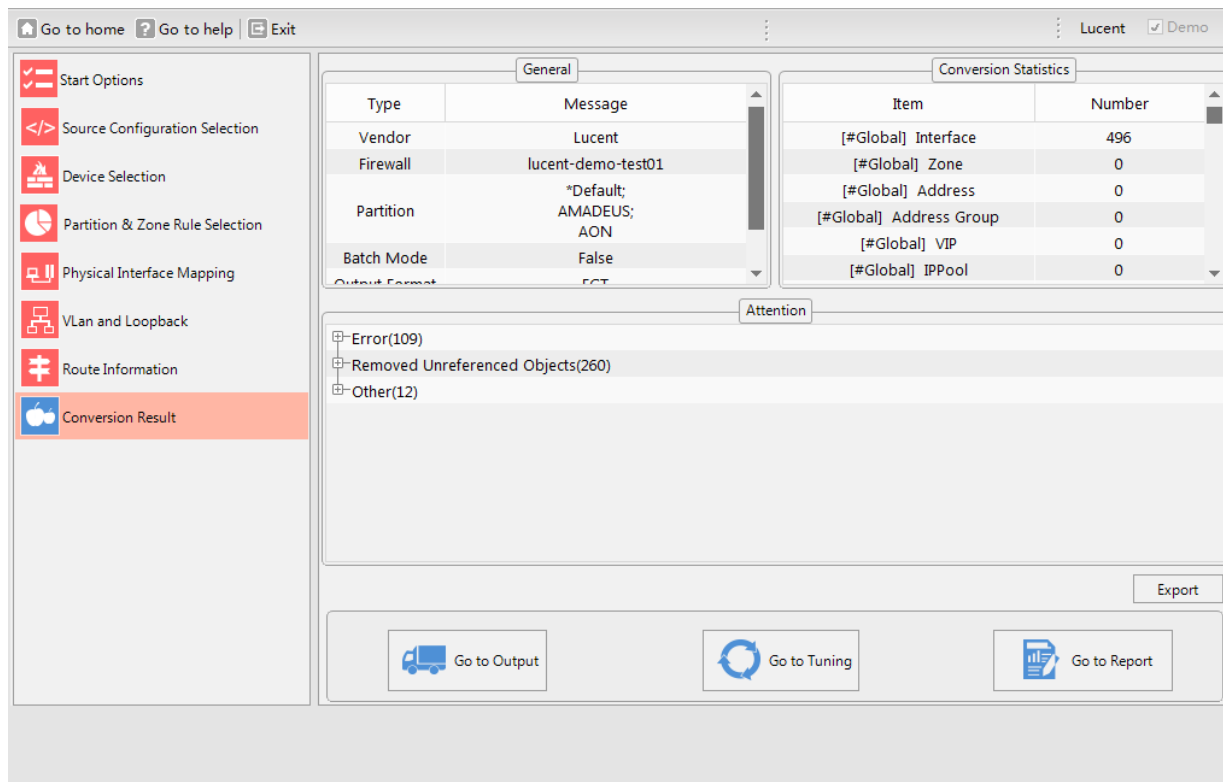
Network	Netmask	Gateway	Interface
*Default			
0.0.0.0	0.0.0.0	66.119.71.41	*Default
vm2m-all-networks	Object Static Route	192.168.181.118	*Default
10.234.138.118	255.255.255.255	10.253.173.18	*Default
santander-PR2Remedy-sources	Object Static Route	10.253.173.18	*Default
10.234.134.0	255.255.255.0	10.253.173.18	*Default
terra-internal	Object Static Route	172.21.237.14	*Default
172.24.0.0	255.255.0.0	10.253.173.82	*Default
192.168.183.0	255.255.255.0	10.253.173.18	*Default
10.253.168.0	255.255.255.128	10.253.173.18	*Default
10.204.0.0	255.254.0.0	10.253.173.82	*Default
10.107.64.0	255.255.192.0	10.253.173.82	*Default
10.28.0.0	255.254.0.0	10.253.173.82	*Default
192.168.36.48	255.255.255.240	172.21.226.177	*Default
10.26.0.0	255.254.0.0	10.253.173.82	*Default
10.225.128.0	255.255.128.0	10.253.173.82	*Default
10.222.0.0	255.254.0.0	10.253.173.82	*Default
10.216.0.0	255.254.0.0	10.253.173.82	*Default
10.202.0.0	255.255.0.0	10.253.173.82	*Default

Add
Edit
Delete

Next >

Setting	Description
Add	Click to add a route.
Edit	Click to edit the selected route.
Delete	Click to delete the selected route.

Conversion Result



Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81 .
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see [Viewing the results of your automatic conversion on page 79](#)

Check Point conversion wizard

The pages that the Check Point conversion wizard displays depend on whether your source configuration is SmartCenter or Provider-1.

Including object comments in the output configuration

By default, output configurations from Check Point do not include:

- comments for interface, address, service, or rule objects
- review memo information for policy objects

To configure FortiConverter to include object comments

1. Before you start the conversion wizard, open the file CheckpointOptions.txt in the FortiConverter installation directory in a plain-text editor. (The default location of the file is C:\Program Files (x86)\Fortinet\FortiConverter\CheckpointOptions.txt.)
2. Remove the # (number sign) from one or more of the following entries to include the corresponding data in the output configuration:


```
#interface comment
#address comment
#service comment
#rule comment
#policy review memo
```
3. Save your changes, and then start the wizard to begin the conversion process.

Start Options

Setting	Description
Model	Select the source Check Point model.
Output Format	Select the appropriate output for your target Fortinet device. You can convert Provider-1 to FortiManager output only.

Setting	Description
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Ignore “all” address match for NAT	Specifies whether FortiConverter ignores addresses with an “all/any” address when it merges a NAT rule and a security rule to create a FortiGate NAT policy. (In most cases, this type of address matches anything.)
Auto generate policy interfaces	Specifies whether FortiConverter generates policy interfaces using the Checkpoint route file.
More	Displays additional start options. See Start Options - More on page 30 .
Output Directory	Select the folder where the output configuration is saved.

Start Options - More

Start Options

Policy conversion options

☒ Discard unreferenced firewall objects Convert 'Day in Month' within year

☐ Auto generate policy interfaces

Comment options

☐ Interface comment ☒ Policy Package Name + Rule Number

☐ Address comment ☐ Original Checkpoint firewall rule comment

☐ Service comment ☐ Policy Package Name + Rule Number + Original Checkpoint firewall rule comment

NAT merge options

☐ Ignore "all" address match for NAT ☐ Generate NAT merge review memo into a separate text file

☐ Enable Central NAT merge

Back

Next >

Setting	Description
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.

Setting	Description
Auto generate policy interfaces	Specifies whether FortiConverter generates policy interfaces using the Check Point route file.
Convert 'Day in Month' within X year	<p>Specifies how many years of one-time schedules to generate.</p> <p>The wizard converts Check Point "day in month" schedules into equivalent one-time FortiGate schedules.</p>
Interface comment	Specifies whether FortiConverter copies the interface comment from the source configuration to the mapped FortiGate interface.
Address comment	Specifies whether FortiConverter copies the address comment from source configuration to the converted FortiGate address.
Service comment	Specifies whether FortiConverter copies the service comment from the source configuration to converted FortiGate service.
Policy Package Name + Rule Number	
Original Check Point firewall rule comment	Specifies what information FortiConverter includes in the converted policy comment.
Policy Package + Rule Number + Original Check Point firewall rule comment	
Ignore "all" address match for NAT	Specifies whether FortiConverter ignores addresses with an "all/any" address when it merges a NAT rule and a security rule to create a FortiGate NAT policy. (In most cases, this type of address matches anything.)
Enable Central NAT merge	Specifies whether FortiConverter converts Hide NATs to FortiGate central NATs instead of a policy-based NATs.
Generate NAT merge review memo as a separate text file	<p>Specifies whether FortiConverter generates a separate text file for NAT merge policies.</p> <p>FortiConverter generates NAT merge policies by merging NAT and security rules in the source configuration.</p>
Back	Displays the main Start Options page.

MDS Source Configuration (Provider-1 only)

Go to home
Go to help
Exit
CheckPoint
Demo

Start Options

MDS Source Configuration

MDS MDS Selection

Global Policy Collection Selection

Domain Source Configuration

Policy Collection Selection

Conversion Result

Hierarchy Definition Files

MDS Definition File (mdss.c) [e.g. ~\mds\opt\CPmds-R76\conf\mdsdb\mdss.c]
C:\Projects\FConv_Releases\Release_0669\demo\CPPProvider-1\mds\opt\CPmds-R76\conf\r
Browse...

MDS Object File(objects_5_0.c) [e.g. ~\mds\opt\CPmds-R76\conf\mdsdb\objects_5_0.c]
C:\Projects\FConv_Releases\Release_0669\demo\CPPProvider-1\mds\opt\CPmds-R76\conf\r
Browse...

Global Policy Definition Files

Global Policy ObjectFile (objects_5_0.c) [e.g. ~\mds\opt\CPmds-R76\conf\objects_5_0.c]
C:\Projects\FConv_Releases\Release_0669\demo\CPPProvider-1\mds\opt\CPmds-R76\conf\r
Browse...

Global Policy Rulebase File (rulebases_5_0.fws) [e.g. ~\mds\opt\CPmds-R76\conf\rulebases_5_0.fws]
C:\Projects\FConv_Releases\Release_0669\demo\CPPProvider-1\mds\opt\CPmds-R76\conf\r
Browse...

Global Policy Assignment File [e.g. ~\mds\opt\CPmds-R76\conf\mdsdb\customer.C]

C:\Projects\FConv_Releases\Release_0669\demo\CPPProvider-1\mds\opt\CPmds-R76\conf\r
Browse...

Next >

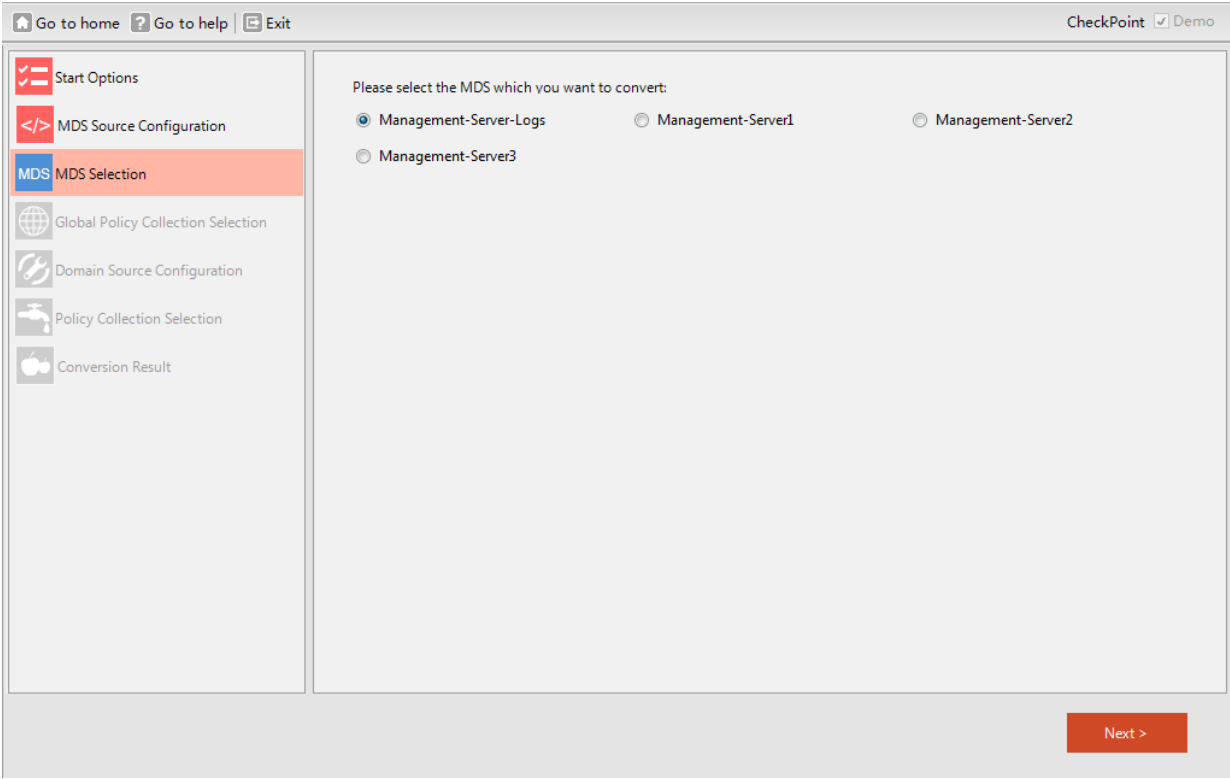
Setting

Description

Browse

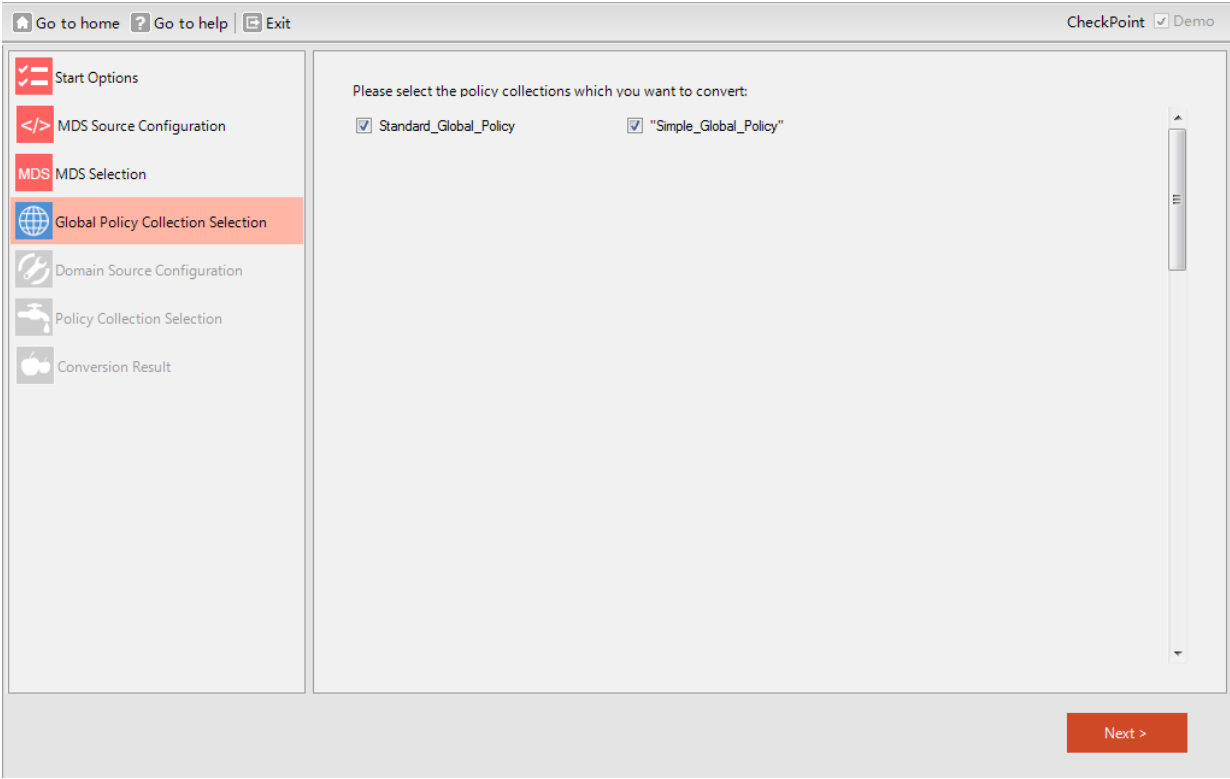
Select the Provider-1 configuration files.

MDS Selection (Provider-1 only)



Setting	Description
Please select the MDS which you want to convert	Select the domain to convert.

Global Policy Collection Selection (Provider-1)



Setting	Description
	Specifies whether FortiConverter converts the Standard Global Policy.
Standard_Global_Policy	You can select both Standard Global Policy and Simple Global Policy .
Simple_Global_Policy	Specifies whether FortiConverter converts the Simple Global Policy.

Domain Source Configuration

Go to homeGo to helpExit

CheckPointDemo

Start Options

Domain Source Configuration

Policy Collection Selection

Firewall Selection

Physical Interface Mapping

Route Information

Conversion Result

Please select the domains which you want to convert and input config files:

SmartCenter

Object Definition File (objects_5_0.C)

Browse...

Policy Information File (Standard.W or rulebases_5_0.fws)

Browse...

[Optional] User and User Groups File (fwauth.NDB)

Browse...

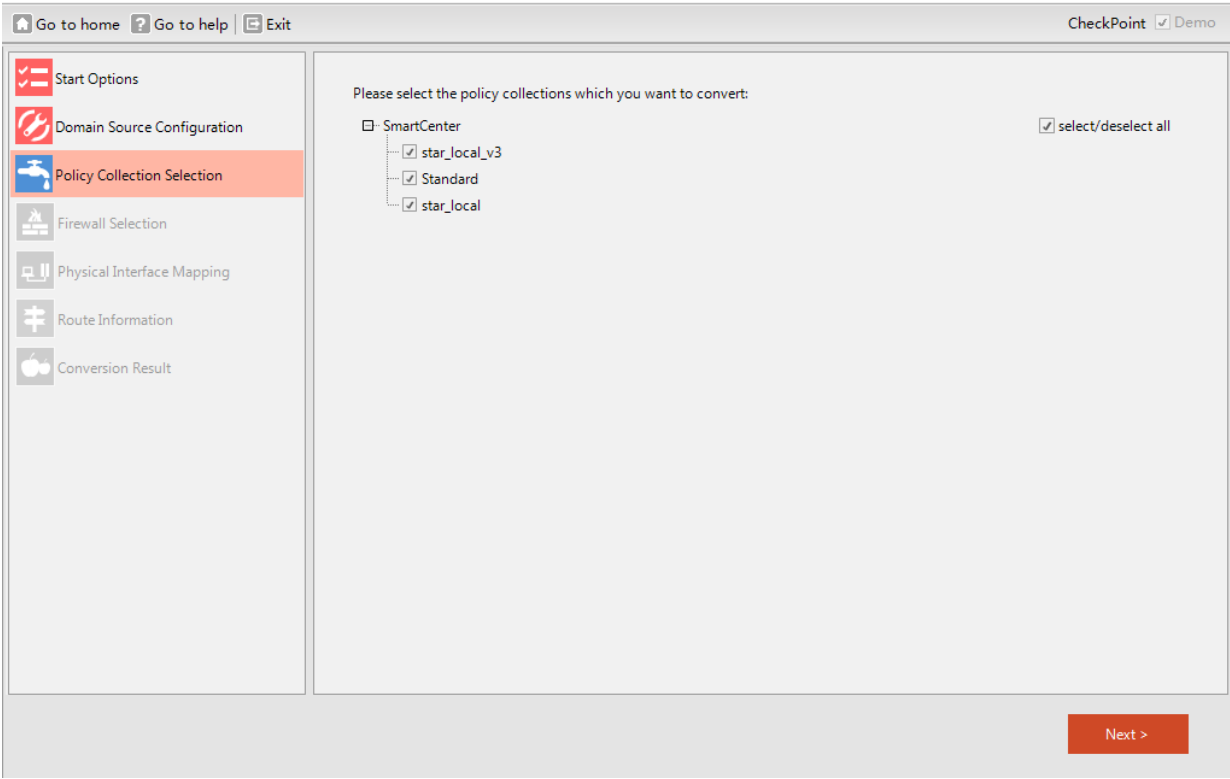
Next >

Setting	Description
	Click to select domain source configuration files.
Browse	For information on acquiring these files, see Downloading the source configuration files on page 17 .

35

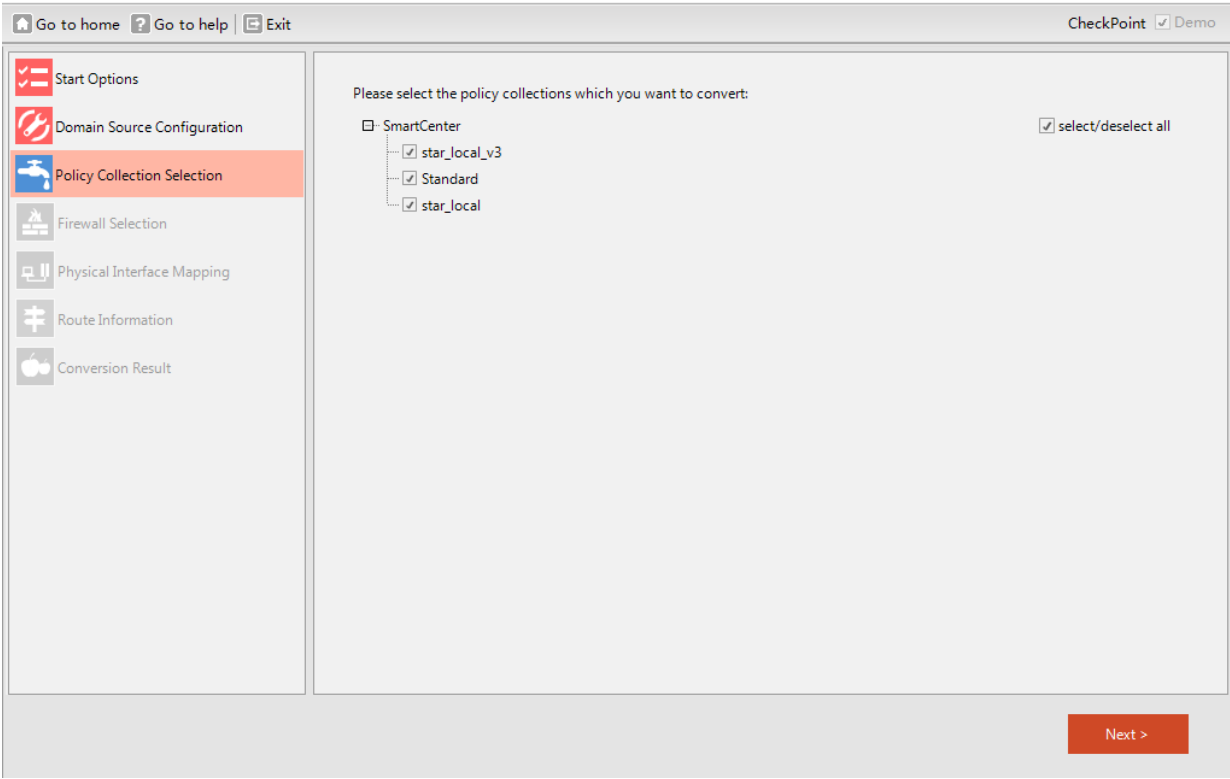
FortiConverter User Guide
Fortinet Technologies Inc.

Policy Collection Selection



Setting	Description
(policy collection item)	Select the policy collections to convert.
Select/deselect all	Select or clear all policy collection items.

Firewall Selection (SmartCenter only)



Setting	Description
Retail Branch Batch Mode	Select to specify multiple firewalls from the list. Select only firewalls with the same interfaces.
(firewall item)	For more information, see Using retail branch batch conversion mode on page 74
Route File	Select one or more firewalls to convert.
	(Optional) Enter the path and file name of a file that contains route information, or click Browse to select it.

Physical Interface Mapping (SmartCenter only)

Go to home
Go to help
Exit
CheckPoint ☒ Demo

Start Options

Domain Source Configuration

Policy Collection Selection

Firewall Selection

Physical Interface Mapping

Route Information

Conversion Result

Physical Interface Mapping

Please click the '?'

Name	IP	Netmask	Alias	Status	FG Port
Lan1	10.231.149.1	255.255.255.0		up	port1
Internal	10.7.42.1	255.255.255.0		up	port2
External	172.29.46.167	255.255.255.0		up	?

Next >

Setting	Description
FG port	Click to assign a FortiGate port for each interface.
(table column)	Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

Route Information (SmartCenter only)

Go to homeGo to helpExit

CheckPointDemo

Start Options

Domain Source Configuration

Policy Collection Selection

Firewall Selection

Physical Interface Mapping

Route Information

Conversion Result

Route Information

Network	Netmask	Gateway	Interface
---------	---------	---------	-----------

AddEditDelete

Next >

Setting	Description
Add	Click to add a route.
Edit	Click to edit the selected route.
Delete	Click to delete the selected route.

Conversion Result

Go to home ? Go to help Exit CheckPoint ☒ Demo

General

Type	Message
Vendor	Checkpoint
Firewall	UTM-1-Cluster-Primary-Member
Rule Base	star_local_v3; Standard; star_local
Batch Mode	False
Output Format	JSON

Conversion Statistics

Item	Number
Interface	3
Zone	0
Address	70
Address Group	20
VIP	0
IPPool	2

Attention

- [-] Unsupported Syntax(18)
- [-] Removed Unreferenced Objects(132)
- [-] Other(4)

Export

Go to Output Go to Tuning Go to Report

Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81 .
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see [Viewing the results of your automatic conversion on page 79](#)

Cisco conversion wizard

Start Options

Setting	Description
Model	Select the model of the source configuration.
Output Format	Select the appropriate output format for your FortiGate device.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Enable NAT merge memo	Specifies whether FortiConverter copies NAT merge policies to a separate text file that you can review. The file name is <code>PolicyMemo.txt</code> .
Set policy comment with source config line	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Auto generate policy interfaces	Specifies whether FortiConverter generates policy interfaces using the Cisco route file.

Setting	Description
Output Directory	Select the folder where the output configuration is saved.

Source Configuration Selection

Home Tuning Help Exit Cisco Demo

☒ Start Options

☒ Source Configuration Selection

☐ Context Selection

☐ Physical Interface Mapping

☐ Route Information

☐ Conversion Result

☐ Retail Branch Batch Mode

Source Configuration File

Browse...

*For Cisco Virtual Context conversion, please input System Execution Space Configuration file, and the file names of individual Contexts should be the same as the records in the input.

Next >

Setting	Description
Retail Branch Batch Mode	Select to specify multiple source configuration files. Ensure that all the source files use the same interface. For more information, see Using retail branch batch conversion mode on page 74
Source Configuration File	Select the input file or files.

Context Selection

The screenshot shows the 'Context Selection' window of the FortiConverter application. The window has a title bar with 'Home', 'Tuning', 'Help', and 'Exit' buttons. On the right side of the title bar, there are 'Cisco' and 'Demo' checkboxes. The main area is divided into two panes. The left pane contains a sidebar with icons and labels: 'Start Options' (checked), 'Source Configuration Selection' (code icon), 'Context Selection' (highlighted with a red background), 'Physical Interface Mapping' (network icon), 'Route Information' (plus icon), and 'Conversion Result' (apple icon). The right pane is titled 'Cisco Multiple Context Selection:' and contains the text 'Admin Context: HOSTNET'. Below this, there is a grid of checkboxes for various contexts:

<input checked="" type="checkbox"/> HOSTNET	<input type="checkbox"/> AIP	<input type="checkbox"/> AIPMO
<input type="checkbox"/> AO	<input type="checkbox"/> AFM	<input type="checkbox"/> INFOLJIN
<input type="checkbox"/> MVG	<input type="checkbox"/> SHARED-S	<input type="checkbox"/> TECH-S
<input type="checkbox"/> VIP	<input type="checkbox"/> VOICE-S	<input type="checkbox"/> VREEMD

 In the top right corner of the right pane, there is a 'Select all' checkbox. At the bottom right of the window, there is a red 'Next >' button.

Select one or more virtual contexts to convert to equivalent VDOMs.

This page is displayed only if you have provided a virtual context input file.

Physical Interface Mapping

Go to home
Go to help
Exit
Cisco
Demo

Start Options
Source Configuration Selection
Physical Interface Mapping
Vlan and Loopback
Route Information
VPN Phase2
Conversion Result

Physical Interface Mapping

Please click the '?'

Name	IP	Netmask	Alias	Status	FG Port
root					
FastEthernet0/0	192.168.99.200	255.255.255.0	inside	up	port1
FastEthernet0/1	172.16.1.100	255.255.255.0	outside	up	port2
FastEthernet1/0	10.0.0.100	255.255.255.0		up	?

Next >

Setting	Description
FG port (table column)	Click to assign a FortiGate port for each interface. Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

VLAN and Loopback

[Go to home](#) [Go to help](#) [Exit](#)

Start Options

Source Configuration Selection

Physical Interface Mapping

Vlan and Loopback

Route Information

VPN Phase2

Conversion Result

VLAN and Loopback Interface

Name	IP	Netmask	Alias	Status
root				
FastEthernet0/0.11	11.0.0.100	255.255.255.0		up
FastEthernet0/0.12	12.0.0.100	255.255.255.0		up
Loopback0	192.168.1.100	255.255.255.255		up

Next >

For information only. No settings.

Route Information

Go to homeGo to helpExit

Start Options

Source Configuration Selection

Physical Interface Mapping

Vlan and Loopback

Route Information

VPN Phase2

Conversion Result

Route Information

Network	Netmask	Gateway	Interface
root			
0.0.0.0	0.0.0.0	172.16.1.1	FastEthernet0/1
172.16.2.0	255.255.255.0	172.16.1.1	FastEthernet0/1
172.18.1.0	255.255.255.0		FastEthernet0/1

Add

Edit

Delete

Next >

Setting	Description
Add	Click to add a route.
Edit	Click to edit the selected route.
Delete	Click to delete the selected route.

VPN Phase2

Go to home

Go to help

Exit

Cisco

☒ Demo

Start Options

Source Configuration Selection

Physical Interface Mapping

Vlan and Loopback

Route Information

VPN Phase2

Conversion Result

VPN Phase2

Please click the '?'

Name	Priority	Dynamic	Peer	Interface	IKE Phase1
root					
test	10		172.16.2.100	FastEthernet0/1	pre-share
test	11		172.16.2.101	FastEthernet0/1	<div><div>?</div><div>pre-share</div><div>rsa-sig</div></div>

Next >

Setting	Description
IKE Phase1 (table column)	Select an IKE Phase1 authentication method: pre-share (preshared keys) or rsa-sig (RSA signatures).

Conversion Result

The screenshot displays the 'Conversion Result' interface. On the left is a sidebar with icons for 'Start Options', 'Source Configuration Selection', 'Physical Interface Mapping', 'Vlan and Loopback', 'Route Information', 'VPN Phase2', and 'Conversion Result' (which is highlighted). The main area has a 'General' tab showing configuration details: Vendor (Cisco), Batch Mode (False), Output Format (FGT), and Date / Time (4/28/2015 7:32:33 PM). To the right is a 'Conversion Statistics' table:

Item	Number
Interface	6
Zone	4
Address	11
Address Group	0
VIP	0
IPPool	0

Below the statistics is an 'Attention' section with a list of conversion failures:

- Conversion Failure(11)
- Removed Unreferenced Objects(4)
- Other(2)

At the bottom right is an 'Export' button. At the bottom are three buttons: 'Go to Output' (with a truck icon), 'Go to Tuning' (with a circular arrow icon), and 'Go to Report' (with a document icon).

Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81 .
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see [Viewing the results of your automatic conversion on page 79](#)

Fortinet conversion wizard

Start Options

The screenshot shows the 'Start Options' window of the Fortinet conversion wizard. It features a sidebar on the left with a 'Start Options' tab. The main content area is divided into several sections for configuration:

- Conversion Mode:** A radio button is selected for 'Convert'.
- Output Format:** A radio button is selected for 'FortiGate'.
- Output OS Version:** Four radio buttons are present: 'Same as input' (selected), 'v 4.3 to 5.0', 'v 5.0 to 5.2', and 'v 4.3 to 5.2'.
- Conversion Option:** Two checkboxes are shown: 'Split VDOMs' and 'Create a restorable config', both of which are currently unchecked.
- Output Directory:** A text input field contains the path 'C:\FortiConverterOutput', and a 'Browse...' button is located to its right.

A 'Next >' button is positioned at the bottom right of the window.

Setting	Description
Conversion Mode	Convert is the only supported task.
Output Format	FortiGate is the only supported output format.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the option that matches the OS to convert to.
Split VDOMs	Create an output configuration for each VDOM.
Create a restorable config	Specify whether FortiConverter generates configuration files that you can restore to the target device directly.
Output Directory	Select the folder where the output configuration is saved.

Source Configuration Selection

Start Options

Source Configuration Selection

VDOM Selection

Physical Interface Mapping

Additional Rule

Conversion Result

Source Configuration File

C:\Program Files (x86)\Fortinet\FortiConverter\demo\Fortinet\FG140T3G_VDOM

Browse...

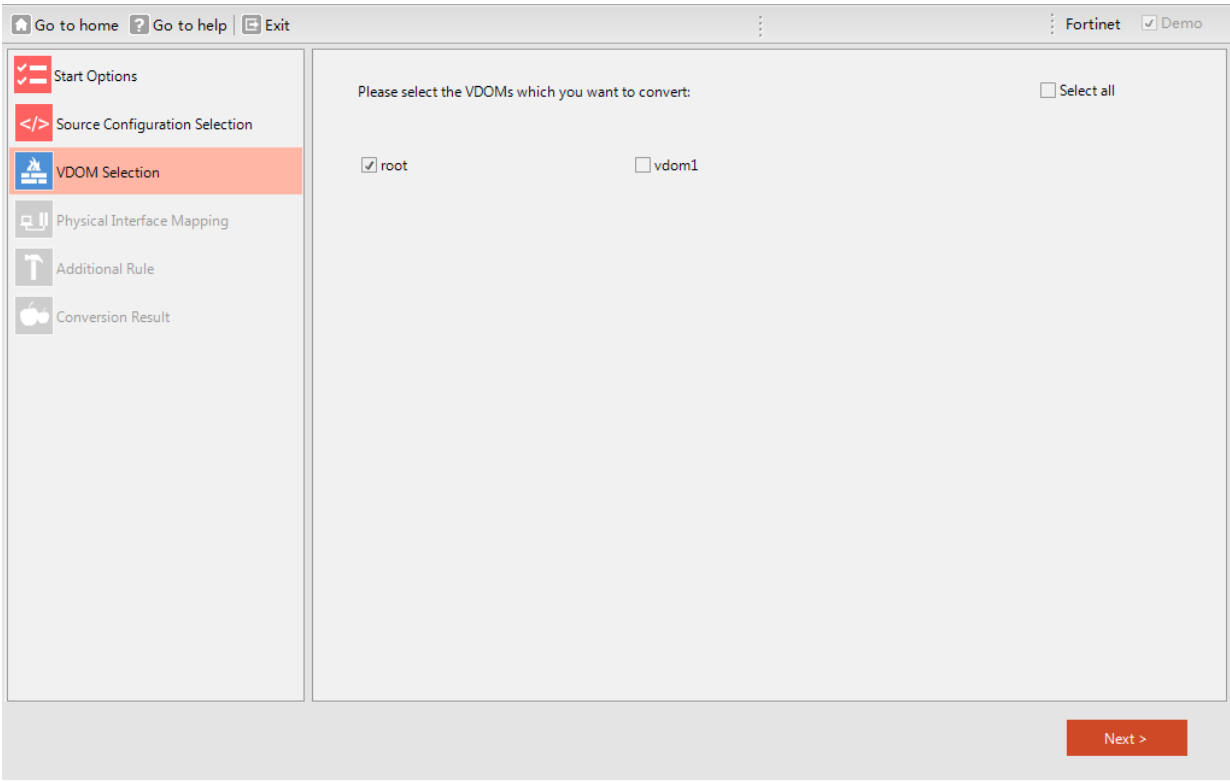
Target Configuration File

Browse...

Next >

Setting	Description
Source Configuration Folder	Select the input folder.
Target Configuration File	Select the target device's default configuration. This is the device configuration before you perform any configuration tasks or after you restore the factory defaults.

VDOM Selection



Setting	Description
Select all	Select to select all VDOMs for conversion.
(VDOM item)	Select one or more VDOMs to convert.

Physical Interface Mapping

Start Options

Source Configuration Selection

VDOM Selection

Physical Interface Mapping

Additional Rule

Conversion Result

Physical Interface Mapping

Please type or select the interface name

Name	IP	Netmask	Alias	Status	FGT Port
root					
"wan2"					port 1
"modem"					port 2
"mgmt"	172.30.144.215	255.255.252.0			Type or select
"ha"					Type or select
"dmz1"	10.10.10.1	255.255.255.0			Type or select
"dmz2"					Type or select
"lan"	192.168.100.99	255.255.255.0			Type or select

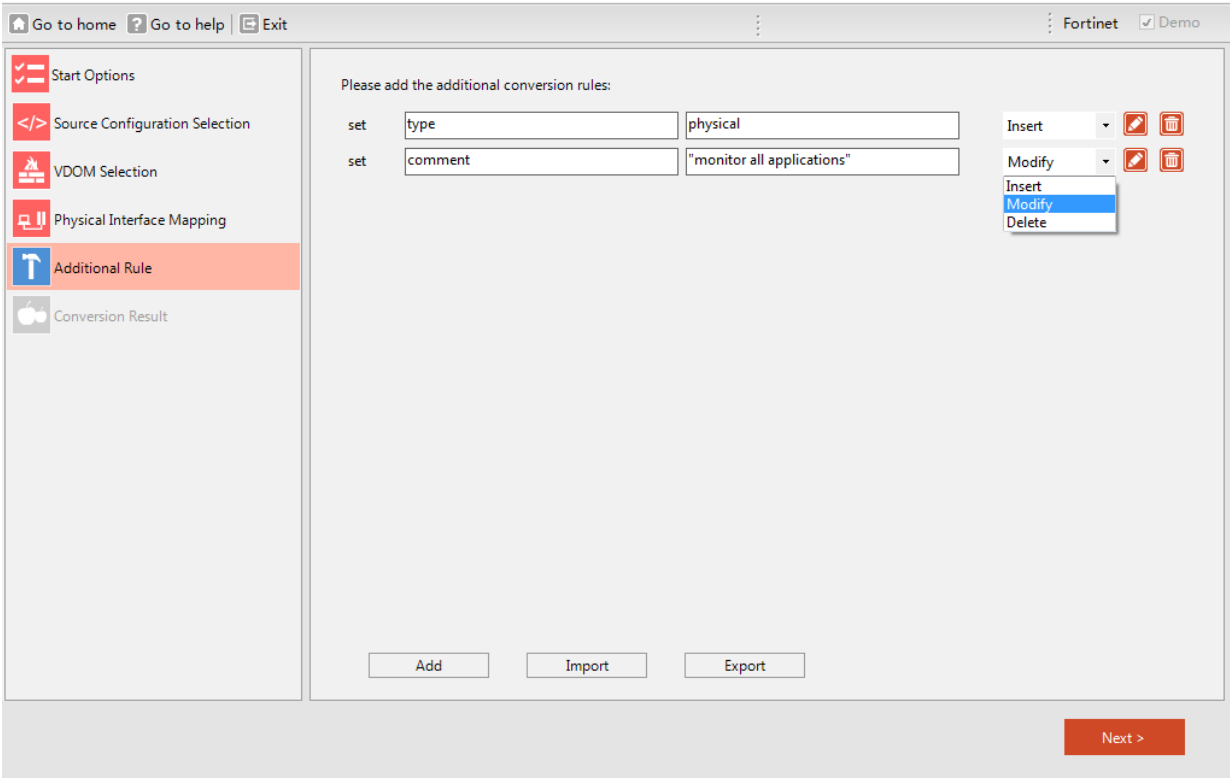
Import

Export

Next >

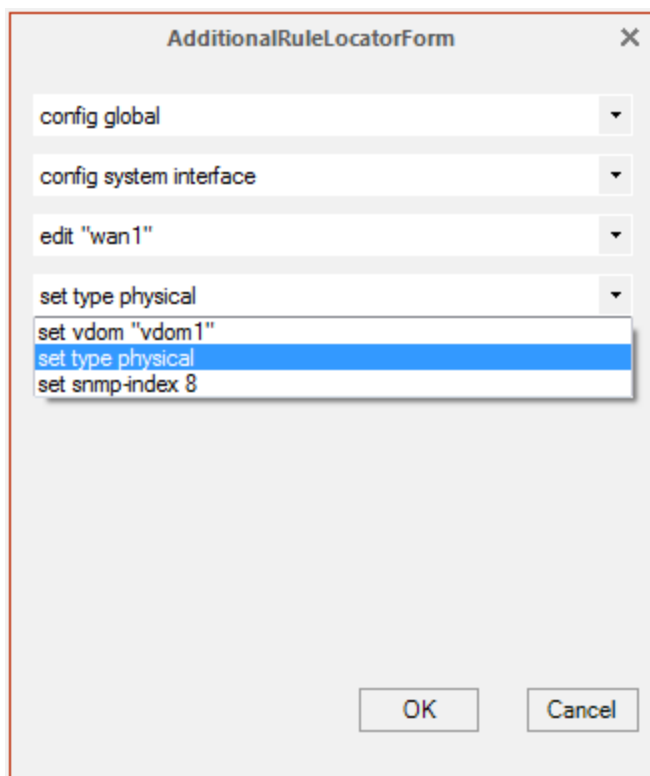
Setting	Description
FG port	Click to assign a FortiGate port for each interface.
(table column)	Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

Additional Rule



Setting	Description
Add	<p>Click to open a dialog box that allows you to select rules from the source configuration to add.</p> <p>See the illustration "Additional rule locator window".</p>
Import	<p>Click to load a set of rule changes from a text file.</p>
Export	<p>Saves the current set of rule changes to a text file.</p>
(rule table)	<ul style="list-style-type: none">Property (first field) – The property of the rule. You can edit this value.Value (second field) – The property's value. You can edit this value.Action (list) – Select either Insert (adds the rule to existing rules), Modify (to change the rule), or Delete.Edit (pencil icon) – Opens the additional rule locator dialog box.Delete (trash can icon) – Removes the rule from the list.

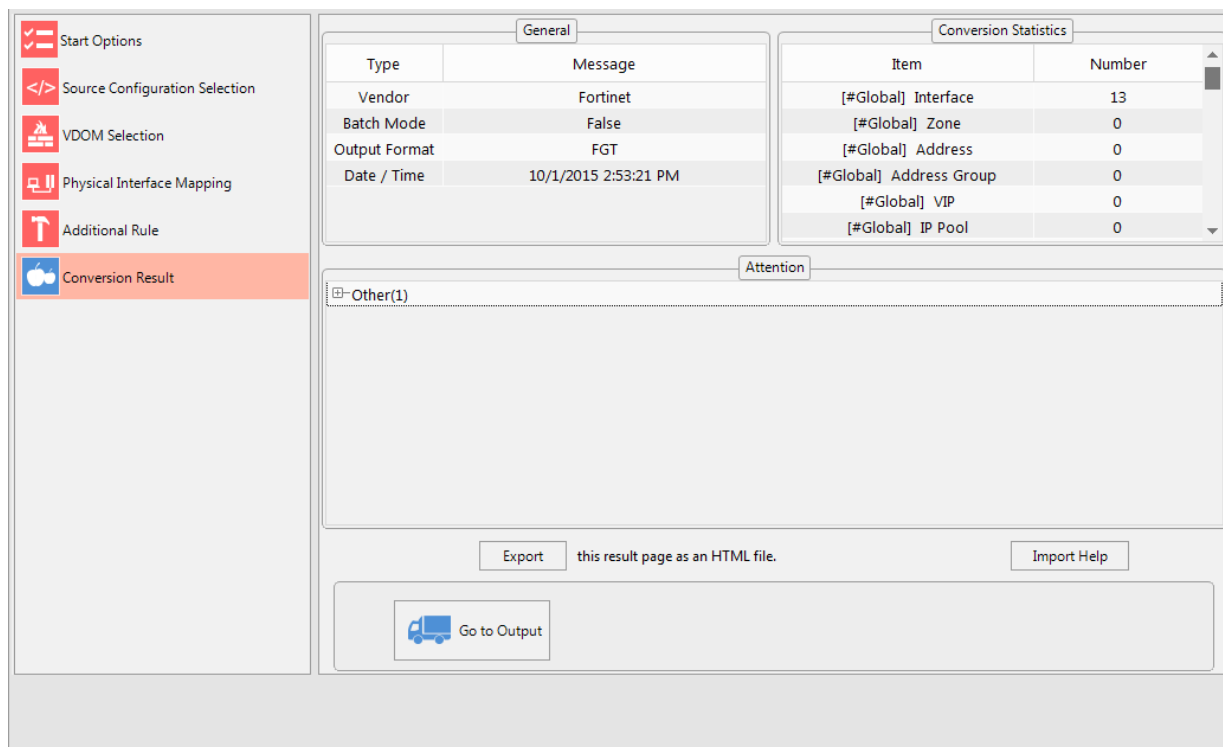
Additional rule locator dialog box



The dialog box, titled "AdditionalRuleLocatorForm", contains a list of configuration commands. The first four are in dropdown menus, and the last three are in a text area. The text area contains the following commands: "set vdom 'vdom1'", "set type physical" (highlighted in blue), and "set snmp-index 8". At the bottom are "OK" and "Cancel" buttons.

Command
config global
config system interface
edit "wan1"
set type physical
set vdom "vdom1"
set type physical
set snmp-index 8

Conversion Result



The "Conversion Result" screen displays the results of the conversion process. It includes a sidebar with navigation options, a "General" tab showing conversion details, a "Conversion Statistics" table, and an "Attention" section with a "Go to Output" button.

Start Options

- Start Options
- Source Configuration Selection
- VDOM Selection
- Physical Interface Mapping
- Additional Rule
- Conversion Result**

General

Type	Message
Vendor	Fortinet
Batch Mode	False
Output Format	FGT
Date / Time	10/1/2015 2:53:21 PM

Conversion Statistics

Item	Number
[#Global] Interface	13
[#Global] Zone	0
[#Global] Address	0
[#Global] Address Group	0
[#Global] VIP	0
[#Global] IP Pool	0

Attention

Other(1)

Export this result page as an HTML file. Import Help

Go to Output

Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
For more information, see Viewing the results of your automatic conversion on page 79	

Juniper conversion wizard

By default, output configurations from Juniper do not include some configuration information, including address and service comments. For an example of how to include this information in the output, see [Including object comments in the output configuration on page 28](#).

Start Options

The screenshot shows the 'Start Options' window of the Juniper conversion wizard. The window has a sidebar on the left with a 'Start Options' button. The main area contains several configuration sections:

- Model:** Two radio buttons, 'SSR/ScreenOS' (selected) and 'SRX/JunOS'.
- Output Format:** Two radio buttons, 'FortiGate' (selected) and 'FortiManager'.
- Output OS Version:** Two radio buttons, 'v 4.x' and 'v5.x' (selected).
- Conversion Option:** Two checkboxes, 'Discard unreferenced firewall objects' (checked) and 'Set policy comment with source config line' (checked).
- Output Directory:** A text box containing 'C:\FortiConverterOutput' and a 'Browse...' button.

At the bottom right, there is a red 'Next >' button.

Setting	Description
Model	Select the model of the source configuration.
Output Format	Select the appropriate output format for your FortiGate device.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.

Setting	Description
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Set policy comment with source config line	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Output Directory	Select the folder where the output configuration is saved.

Source Configuration Selection

Go to home ? Go to help Exit Juniper ☒ Demo

☒ Start Options

</> Source Configuration Selection

☐ LSys Selection

☐ Physical Interface Mapping

☐ Route Information

☐ Conversion Result

☐ Retail Branch Batch Mode

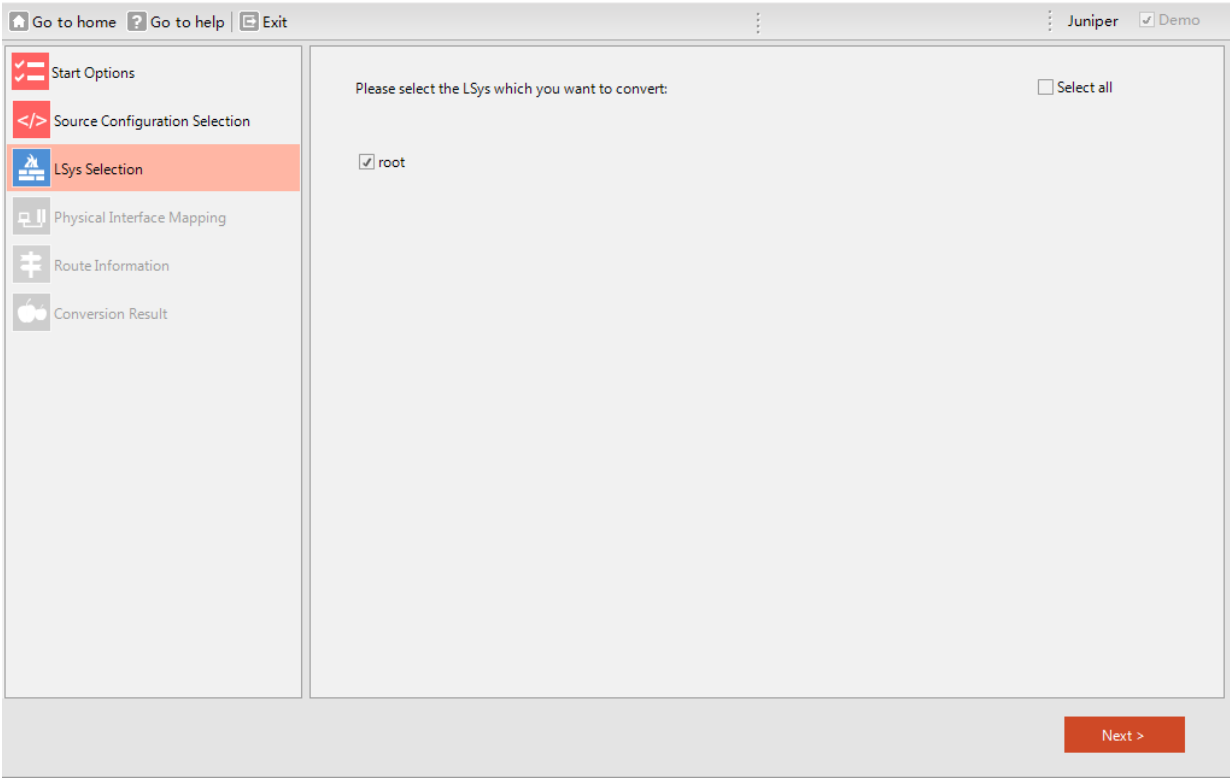
Source Configuration File

C:\Projects\FConv_Releases\Release_0669\demo\juniper-screensos.txt Browse...

Next >

Setting	Description
Retail Branch Batch Mode	Select to specify multiple source configuration files. Ensure that all the source files use the same interface. For more information, see Using retail branch batch conversion mode on page 74
Source Configuration File	Select the input file or files.

LSYS (Junos OS) or VSYS (ScreenOS) Selection



Setting	Description
Select all	Selects or clears all logical virtual system items.
(LSYS or VSYS items)	Select the virtual logical systems to convert.

Physical Interface Mapping

Go to home

Go to help

Exit

Juniper

☒ Demo

Start Options

Source Configuration Selection

LSys Selection

Physical Interface Mapping

Route Information

Conversion Result

Physical Interface Mapping

Please click the '?'

Name	IP	Netmask	Alias	Status	FG Port
root					
ethemet 1	172.22.2.254	255.255.255.0		up	port 1
ethemet2	172.22.1.254	255.255.255.0		up	port2
ethemet3	10.10.10.149	255.255.255.240		up	?

Import

Export

Next >

Setting	Description
FG port	Click to assign a FortiGate port for each interface.
(table column)	Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

Route Information

Go to homeGo to helpExit

Start Options

Source Configuration Selection

LSys Selection

Physical Interface Mapping

Route Information

Conversion Result

Route Information

Network	Netmask	Gateway	Interface
root			
100.2.24.0	255.255.255.0	172.22.2.253	ethernet1
0.0.0.0	0.0.0.0	10.10.10.158	ethernet3
100.2.3.0	255.255.255.0	172.22.2.253	ethernet1
100.2.4.0	255.255.255.0	172.22.2.253	ethernet1
100.2.5.0	255.255.255.0	172.22.2.253	ethernet1
100.2.7.0	255.255.255.0	172.22.2.253	ethernet1
100.2.29.0	255.255.255.0	172.22.2.253	ethernet1

Add

Edit

Delete

Next >

Setting	Description
Add	Click to add a route.
Edit	Click to edit the selected route.
Delete	Click to delete the selected route.

Conversion Result

The screenshot shows the 'Conversion Result' window of the Juniper conversion wizard. The interface is divided into several sections:

- Top Bar:** Contains navigation links: 'Go to home', 'Go to help', and 'Exit'. On the right, it shows 'Juniper' and a checked 'Demo' checkbox.
- Left Sidebar:** A list of navigation options with icons: 'Start Options', 'Source Configuration Selection', 'VSys Selection', 'Physical Interface Mapping', 'Route Information', and 'Conversion Result' (which is highlighted in orange).
- Main Content Area:**
 - General Tab:** A table with two columns: 'Type' and 'Message'.

Type	Message
Vendor	Juniper
Logical System	root
Batch Mode	False
Output Format	FGT
Date / Time	4/28/2015 7:50:11 PM
 - Conversion Statistics Tab:** A table with two columns: 'Item' and 'Number'.

Item	Number
Interface	3
Zone	6
Address	7
Address Group	3
VIP	1
IPPool	0
 - Attention Tab:** A section titled 'Removed Unreferenced Objects(17)' with a large empty box below it.
- Bottom Section:** Contains three buttons: 'Go to Output' (with a truck icon), 'Go to Tuning' (with a circular arrow icon), and 'Go to Report' (with a document icon). An 'Export' button is also present in the top right of this section.

Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81 .
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see [Viewing the results of your automatic conversion on page 79](#)

Palo Alto conversion wizard

Start Options

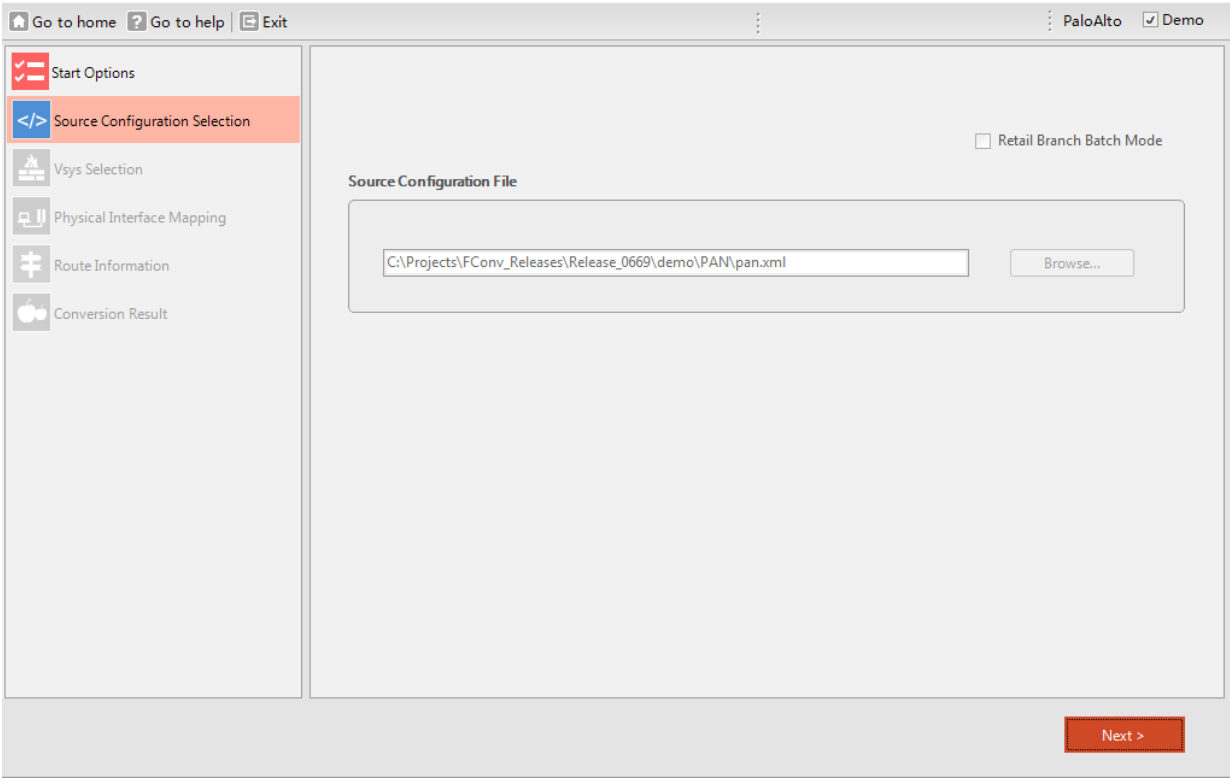
The screenshot shows the 'Start Options' window of the Palo Alto conversion wizard. The window has a title bar with 'Go to home', 'Go to help', and 'Exit' buttons. The sidebar on the left has a 'Start Options' button. The main area contains the following settings:

- Model:** A radio button selection with 'PaloAlto' selected.
- Output Format:** A radio button selection with 'FortiGate' selected.
- Output OS Version:** Radio button selection with 'v 4.x' and 'v5.x'. 'v5.x' is selected.
- Conversion Option:** Two checkboxes: 'Discard unreferenced firewall objects' (checked) and 'Set policy comment with source config line' (checked).
- Output Directory:** A text field containing 'C:\FortiConverterOutput' and a 'Browse...' button.

A 'Next >' button is located at the bottom right of the window.

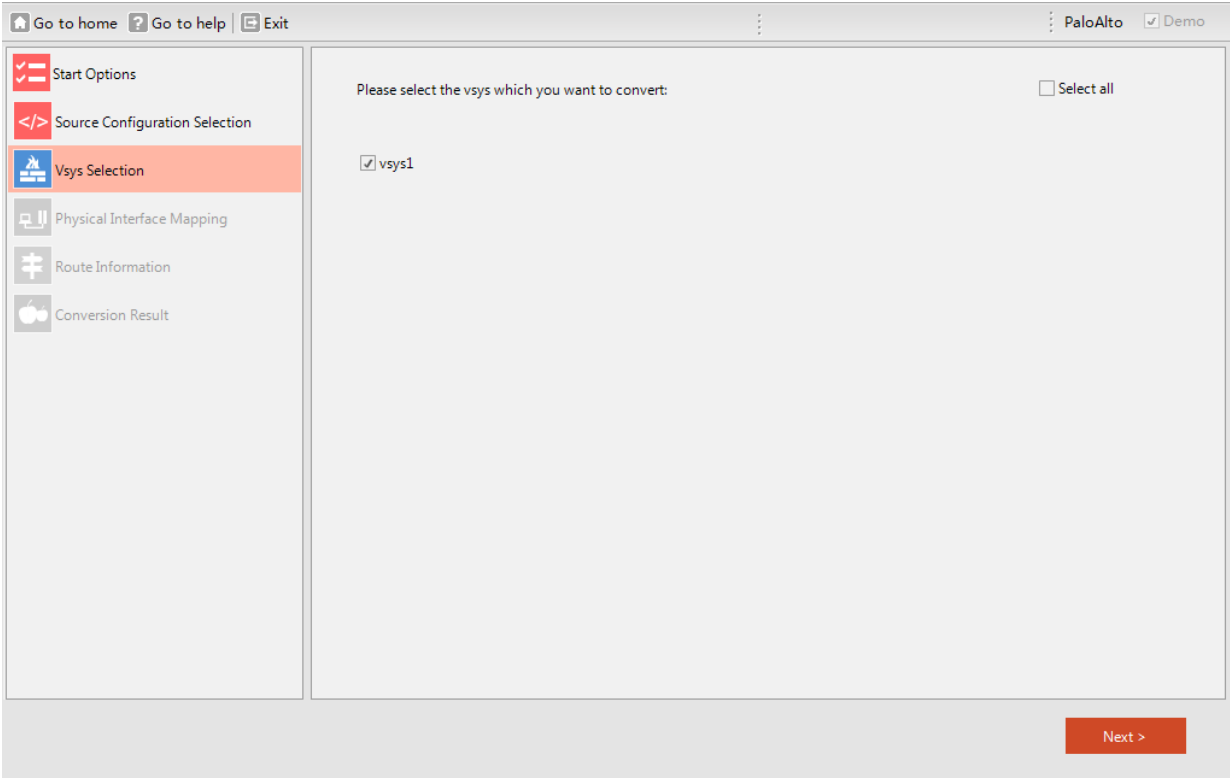
Setting	Description
Model	Palo Alto is the only model supported..
Output Format	FortiGate is the only supported output.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Set policy comment with source config line	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Output Directory	Select the folder where FortiConverter saves the output configuration.

Source Configuration Selection



Setting	Description
Retail Branch Batch Mode	Select to specify multiple source configuration files. Ensure that all the source files use the same interface. For more information, see Using retail branch batch conversion mode on page 74
Source Configuration File	Select the input file or files.

VSYS Selection



Setting	Description
Select all	Selects or clears all virtual system items.
(VSYS items)	Select the virtual systems to convert.

Physical Interface Mapping

Go to home
Go to help
Exit

PaloAlto
Demo

Start Options

Source Configuration Selection

Vsys Selection

Physical Interface Mapping

Conversion Result

Physical Interface Mapping
Please click the '?'

Name	IP	Netmask	Alias	Status	FG Port
vsys1					
ethernet1/2				up	port1
ethernet1/1				up	port2
ethernet1/5	10.200.31.254	255.255.255.0		up	?
ethernet1/7	10.201.31.254	255.255.255.0		up	?
ethernet1/9	10.202.31.254	255.255.255.0		up	?
ethernet1/6	10.200.41.254	255.255.255.0		up	?
ethernet1/8	10.201.41.254	255.255.255.0		up	?
ethernet1/10	10.202.41.254	255.255.255.0		up	?
ethernet1/15	192.168.50.1	255.255.255.0		up	?
ethernet1/16	192.168.51.1	255.255.255.0		up	?
ethernet1/4	22.22.22.1	255.255.255.0		up	?
ethernet1/3	172.30.63.18	255.255.252.0		up	?
ethernet1/19				up	?
ethernet1/20				up	?

Import
Export

Next >

Setting

Description

FG port

Click to assign a FortiGate port for each interface.

(table column)

Enter a port name or custom text.

Import

Click to load a set of interface mappings from a text file.

Export

Saves the current set of interface mappings to a text file.

Conversion Result

Go to home ? Go to help Exit PaloAlto Demo

Start Options

Source Configuration Selection

Vsys Selection

Physical Interface Mapping

Conversion Result

General

Type	Message
Vendor	PAN
Batch Mode	False
Output Format	FGT

Conversion Statistics

Item	Number
[vsys1] Interface	14
[vsys1] Zone	8
[vsys1] Address	0
[vsys1] Address Group	0
[vsys1] VIP	0
[vsys1] IPPool	0

Attention

Export

Go to Output

Go to Tuning

Go to Report

Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81 .
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see [Viewing the results of your automatic conversion on page 79](#)

SonicWall conversion wizard

By default, output configurations from SonicWall do not include some configuration information, including address and service comments. For an example of how to include this information in the output, see [Including object comments in the output configuration on page 28](#).

Start Options

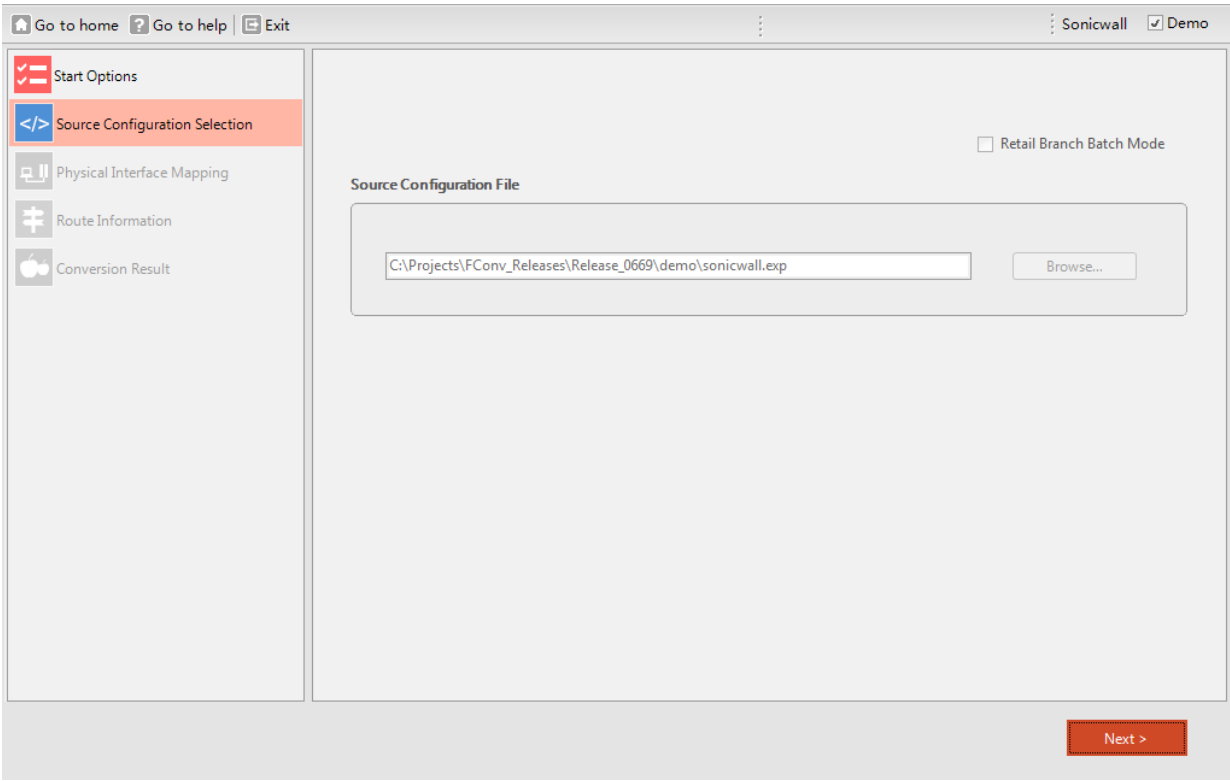
The screenshot shows the 'Start Options' window of the SonicWall conversion wizard. The window has a sidebar on the left with a menu icon and the text 'Start Options'. The main content area is divided into several sections:

- Model:** A radio button selection with 'SonicOS' selected.
- Output Format:** Two radio buttons, 'FortiGate' (selected) and 'FortiManager'.
- Output OS Version:** Two radio buttons, 'v 4.x' and 'v5.x' (selected).
- Conversion Option:** Two checkboxes, both checked: 'Discard unreferenced firewall objects' and 'Set policy comment with source config line'.
- Output Directory:** A text input field containing 'C:\FortiConverterOutput' and a 'Browse...' button.

At the bottom right of the window is a red button labeled 'Next >'.

Setting	Description
Model	SonicOS is the only model supported.
Output Format	Select the appropriate output format for your FortiGate device.
Output OS Version	FortiOS 4.x and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Discard unreferenced firewall objects	Specifies whether addresses, schedules, and services that are not referenced by a policy are saved and added to the output.
Set policy comment with source config line	Specifies whether FortiConverter includes the input configuration lines used for each FortiGate policy in the FortiGate configuration as a policy comment.
Output Directory	Select the folder where FortiConverter saves the output configuration.

Source Configuration Selection



Setting	Description
Retail Branch Batch Mode	Select to specify multiple source configuration files. Ensure that all the source files use the same interface. For more information, see Using retail branch batch conversion mode on page 74
Source Configuration File	Select the input file or files.

Physical Interface Mapping

Go to home
Go to help
Exit
Sonicwall
Demo

Start Options
Source Configuration Selection
Physical Interface Mapping
Vlan and Loopback
Route Information
Conversion Result

Physical Interface Mapping

Please click the '?'

Name	IP	Netmask	Alias	Status	FG Port
root					
X0	10.50.168.17	255.255.255.192		enable	port 1
X1	192.168.0.2	255.255.255.0		enable	port 2
X2	192.168.171.2	255.255.255.0		enable	?
X3				enable	?
X4				enable	?
X5				enable	?
U0				enable	?
U1				enable	?

Import
Export

Next >

Setting	Description
FG port	Click to assign a FortiGate port for each interface.
(table column)	Enter a port name or custom text.
Import	Click to load a set of interface mappings from a text file.
Export	Saves the current set of interface mappings to a text file.

VLAN and Loopback

[Go to home](#) [Go to help](#) [Exit](#)

Sonicwall ☒ Demo

Start Options

Source Configuration Selection

Physical Interface Mapping

VLAN and Loopback

Route Information

Conversion Result

VLAN and Loopback Interface

Name	IP	Netmask	Alias	Status
root				
X3-V7	192.168.33.1	255.255.255.192		enable
X3-V9	172.25.14.1	255.255.255.0		enable
X3-V10	192.168.200.5	255.255.255.0		enable
X3-V20	192.168.6.1	255.255.255.0		enable
X3-V50	172.16.32.1	255.255.255.0		enable
X3-V51	172.16.40.1	255.255.255.0		enable
X3-V52	172.16.33.1	255.255.255.0		enable
X3-V53	172.16.34.1	255.255.255.0		enable
X3-V1	10.10.10.1	255.255.255.0		enable
X3-V3	192.168.4.1	255.255.255.0		enable

Next >

For information only. No settings.

Route Information

Go to homeGo to helpExit

SonicwallDemo

Start Options

Source Configuration Selection

Physical Interface Mapping

VLAN and Loopback

Route Information

Conversion Result

Route Information

Network	Netmask	Gateway	Interface
root			
64.8.70.55	255.255.255.255	192.168.0.1	X1
71.74.56.22	255.255.255.255	75.185.112.1	X4
0.0.0.0	0.0.0.0		

Add

Edit

Delete

Next >

Setting	Description
Add	Click to add a route.
Edit	Click to edit the selected route.
Delete	Click to delete the selected route.

Conversion Result

The screenshot displays the 'Conversion Result' window of the SonicWall conversion wizard. The sidebar on the left contains the following options: Start Options, Source Configuration Selection, Physical Interface Mapping, Vlan and Loopback, Route Information, and **Conversion Result** (highlighted). The main content area has two tabs: 'General' and 'Conversion Statistics'. The 'General' tab shows a table with the following data:

Type	Message
Vendor	Sonicwall
Batch Mode	False
Output Format	FGT
Date / Time	4/28/2015 7:59:06 PM

The 'Conversion Statistics' tab shows a table with the following data:

Item	Number
Interface	23
Zone	9
Address	35
Address Group	9
VIP	0
IPPool	2

Below these tabs is an 'Attention' section with a list of errors:

- [-] Unsupported Syntax(2)
- [-] Removed Unreferenced Objects(108)
- [-] Other(5)

At the bottom of the window, there are three buttons: 'Go to Output' (with a folder icon), 'Go to Tuning' (with a circular arrow icon), and 'Go to Report' (with a document icon). An 'Export' button is also present in the top right of the main content area.

Setting	Description
Export	Generates an HTML page of the conversion result.
Go to Output	Opens the output folder .
Go to Tuning	Opens the tuning page. See Tuning the FortiConverter output on page 81 .
Go to Report	Opens a detailed conversion report that includes a list of converted objects and policies and displays lines from the source configuration that FortiConverter did not convert.

For more information, see [Viewing the results of your automatic conversion on page 79](#)

Snort conversion wizard

Start Options

Go to home | Go to help | Exit

Snort ☐ Demo

Start Options

Rule Variables

Conversion Result

Output FortiOS Version

☐ v2.x ☐ v3.x ☒ v4.x - v5.x

Snort Rules

Conversion Options

☐ Convert annotated rules as "status disable"

Snort Variable Definition(e.g. snort.conf) [Optional]

Output Directory

Setting	Description
Output FortiOS Version	FortiOS 2.x, 4.x, and 5.x have different configuration syntaxes. Select the version that corresponds to the FortiOS version on the target.
Snort Rules	Select the input file.
Convert annotated rules as "status disable"	Select to disable rules that are annotated in the source configuration.
Snort Variable Definition	Optionally, select the Snort variable definition file (for example, <code>snort.conf</code>)
Output Directory	Select the folder where FortiConverter saves the output configuration.

Rule Variables

Go to home

Go to help

Exit

Short ☒ Demo

Start Options

Rule Variables

Conversion Result

IP Variables

	Name	Value
0	EXTERNAL_NET	any
1	HOME_NET	any

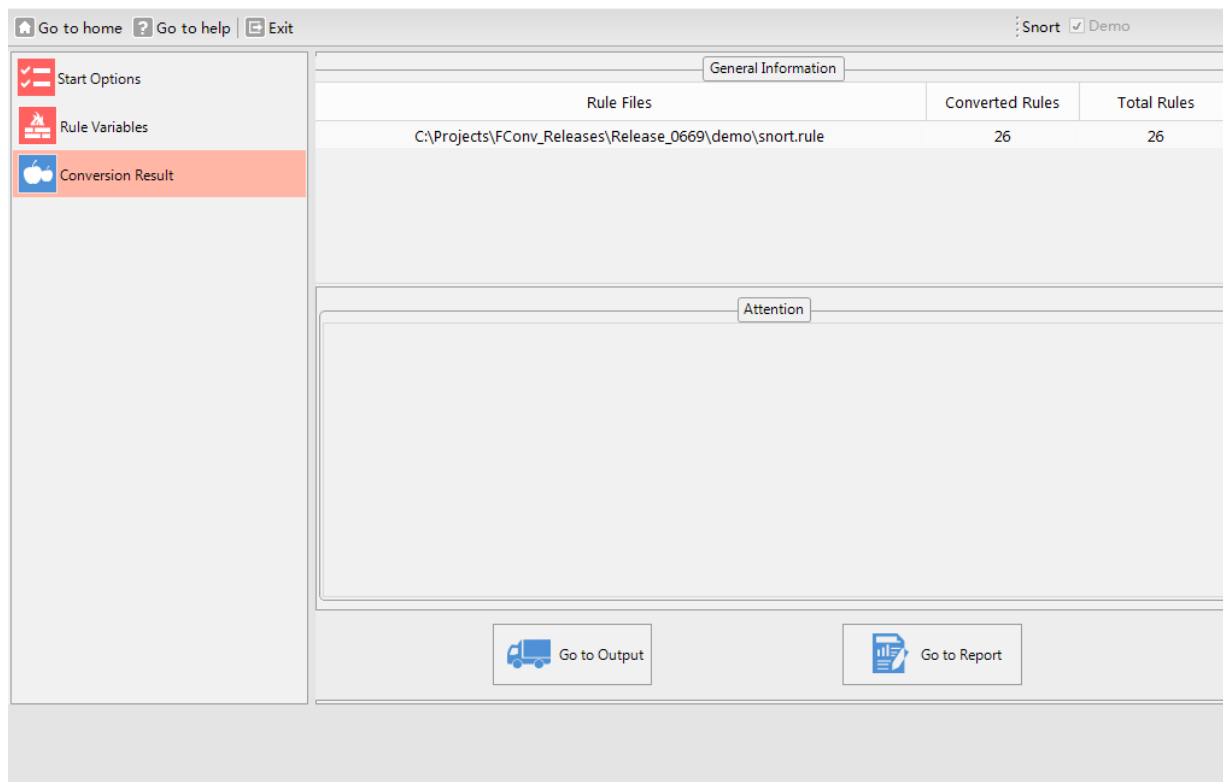
Port Variables

	Name	Value
0	HTTP_PORTS	any

Next >

Setting	Description
IP Variables	Click a value to edit it, if required.
Port Variables	Click a value to edit it, if required.

Conversion Result



Setting	Description
---------	-------------

Go to Output Opens the output folder .

Go to Report Opens an HTML page that displays the conversion mapping.

For more information, see [Viewing the results of your automatic conversion on page 79](#)

Using retail branch batch conversion mode

In the retail industry and other sectors, enterprises often deploy the same firewall configuration at a large number of remote sites. Instead of converting each site individually, the FortiConverter **Retail Branch Batch Mode** option allows you to use the wizard to convert all these sites in a single operation.

Typically, these firewall configurations have one or two network interfaces that connect to a WAN and differ only in the specified LAN and WAN IP addresses, the device name, and a few configuration objects.

Because the batch mode converts the specified group of configurations to a FortiGate configuration with a standard interface mapping, it requires that all the source configurations have the same number of network interfaces. The wizard applies the **FG Port** values that you specify in the wizard's physical port mapping settings to all the output configurations. If any of the source configurations you select have a different number of interfaces, the wizard displays an alert.

Most of the conversion wizard steps are the same as when you convert a single configuration. However, the fine tuning feature you can use to edit the conversion configuration is not available in batch mode.

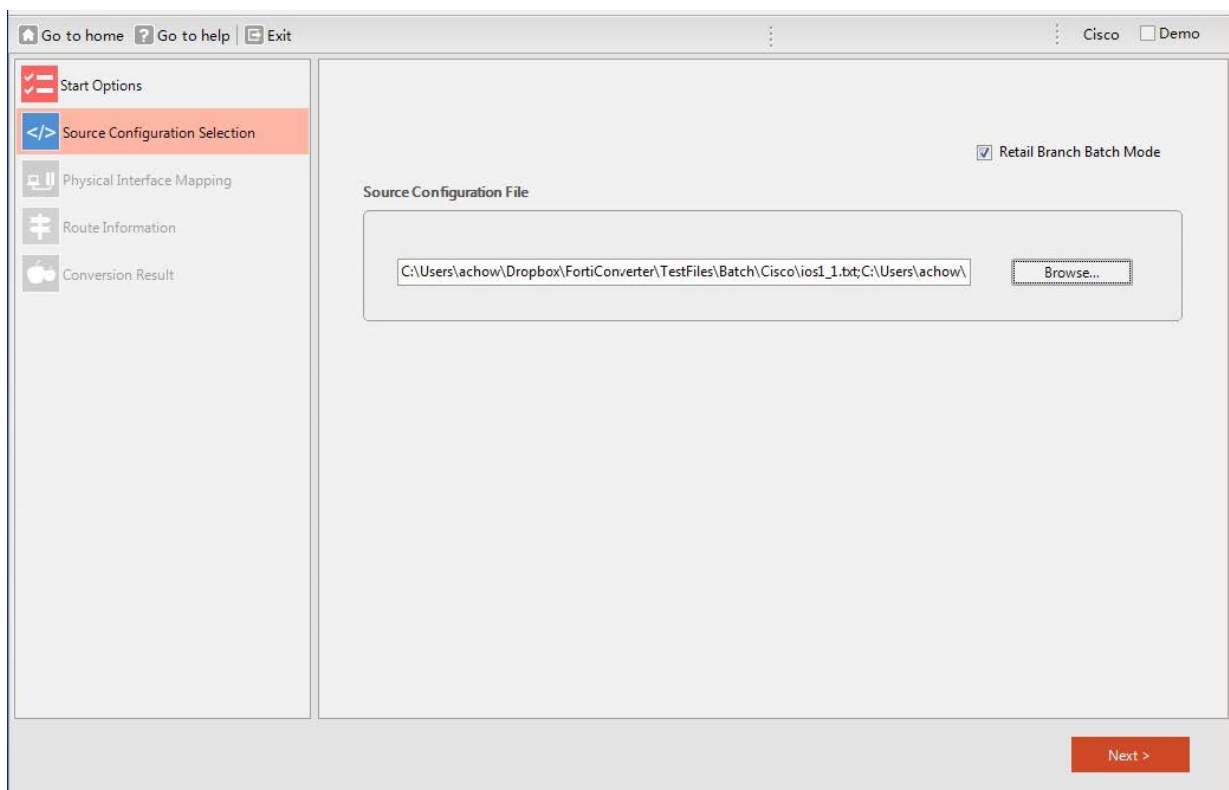
If any of your sites has a unique configuration or needs to be customized (for example, a firewall at the head office), do not use the **Retail Branch Batch Mode** option. Instead, see the instructions for converting a single configuration for your source firewall.

Batch mode for Cisco, Juniper, Palo Alto Networks, and SonicWall firewalls

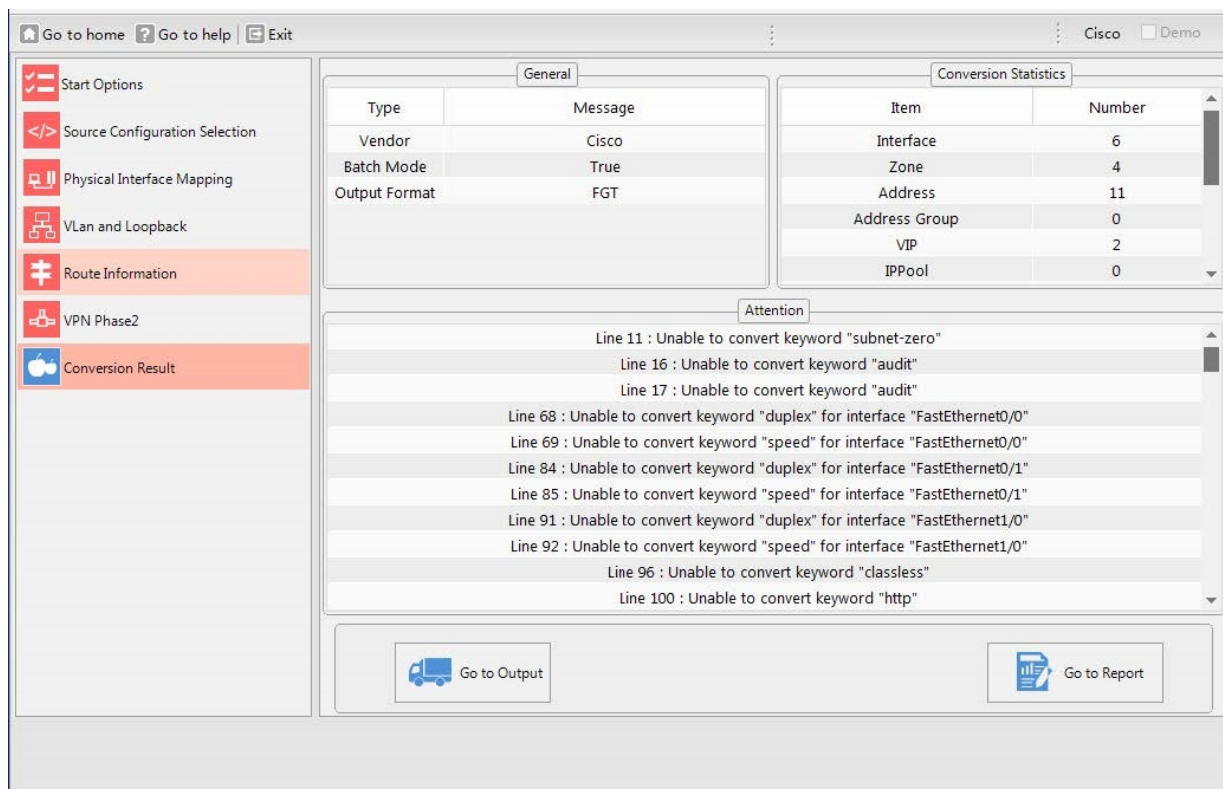
To enable batch mode when you convert Cisco, Juniper, Palo Alto Networks, and SonicWall firewalls, on the wizard's Source Configuration Selection page, select **Retail Branch Batch Mode**.

Click **Browse** to navigate to and select the configuration files. You can select multiple files.

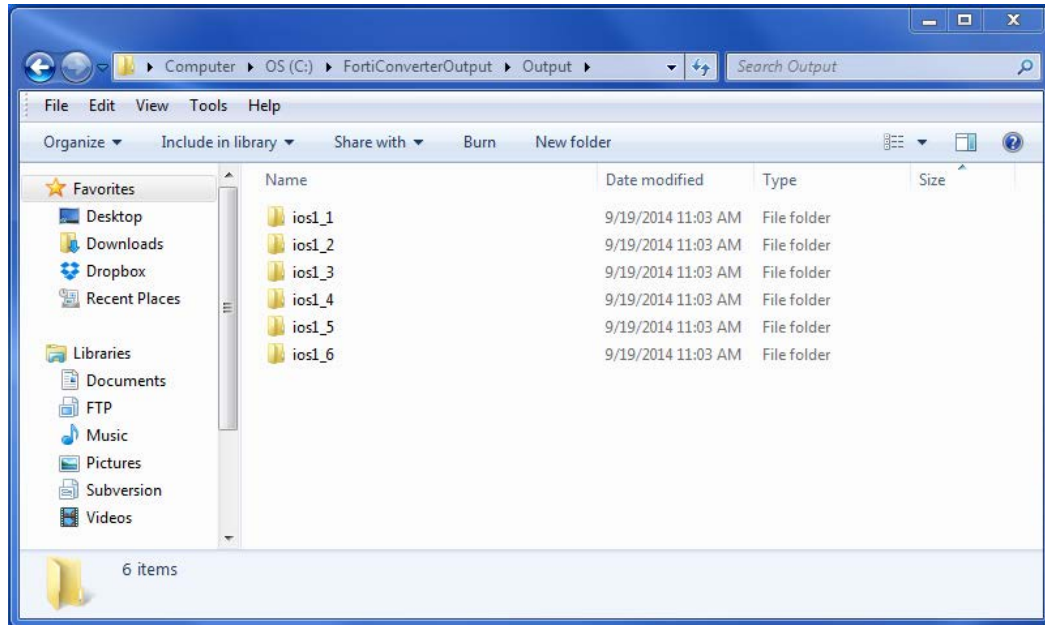
The wizard displays the selected files in a single line in the **Source Configuration File** field.



All other steps for using the wizard are the same as when you convert a single configuration, except for the **Conversion Result** page, which does not display the **Go to Tuning** option.



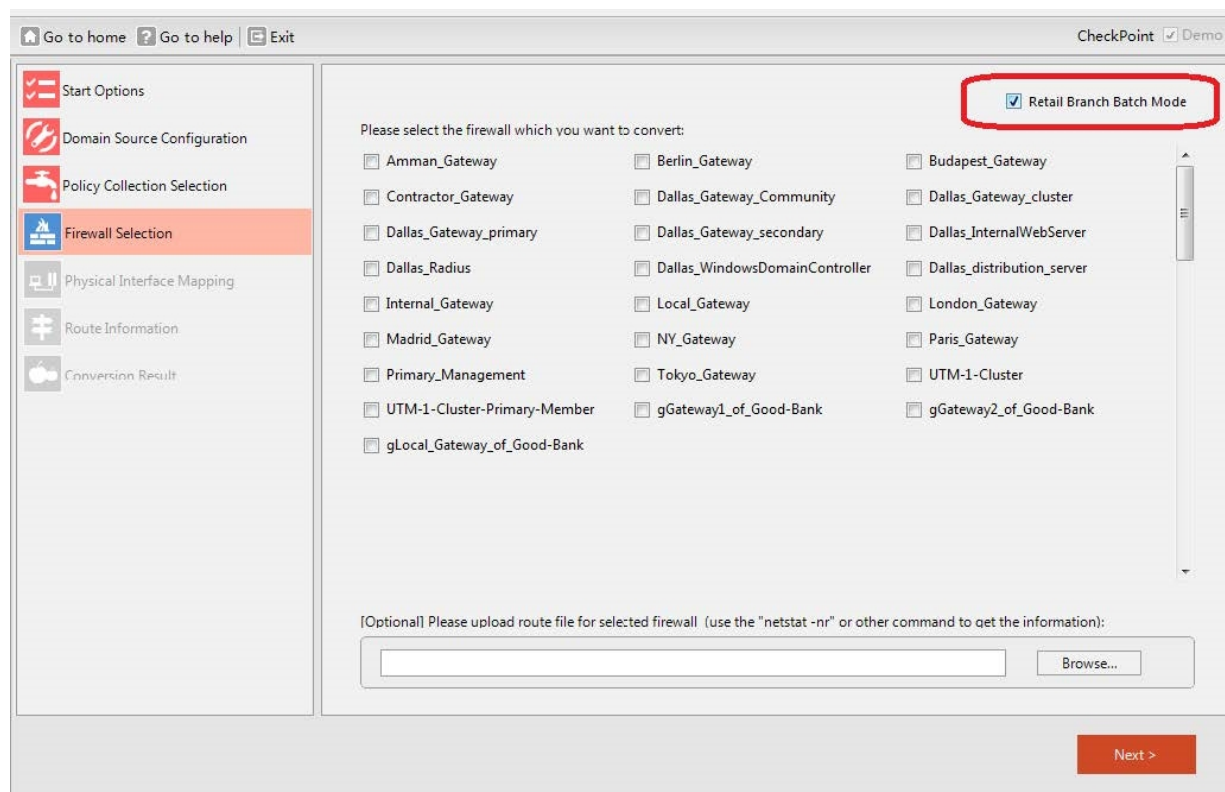
For batch conversion, the wizard saves each configuration file in its own directory in the output directory.



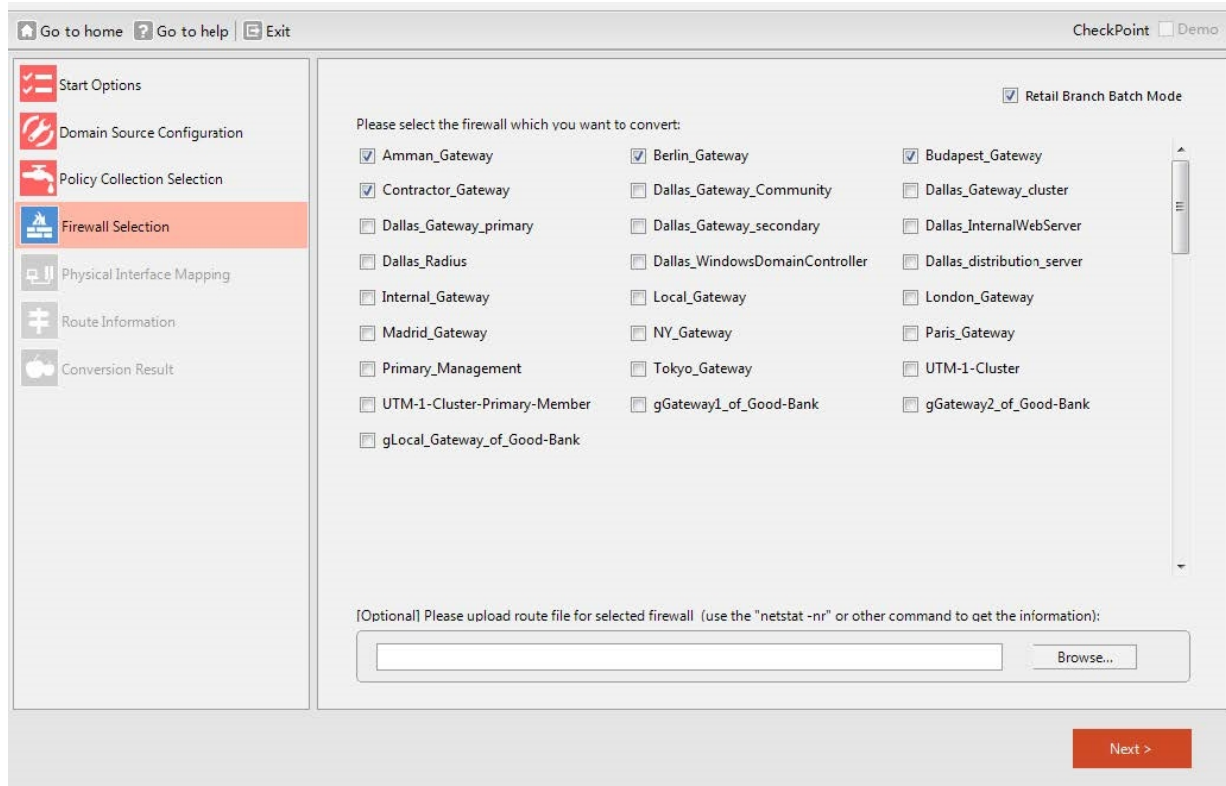
Batch mode for Alcatel-Lucent and Check Point firewalls

For Check Point and Alcatel-Lucent firewalls, batch mode can convert multiple firewalls within a configuration. You select the same input configuration and output settings as when you convert a single configuration. Then, on

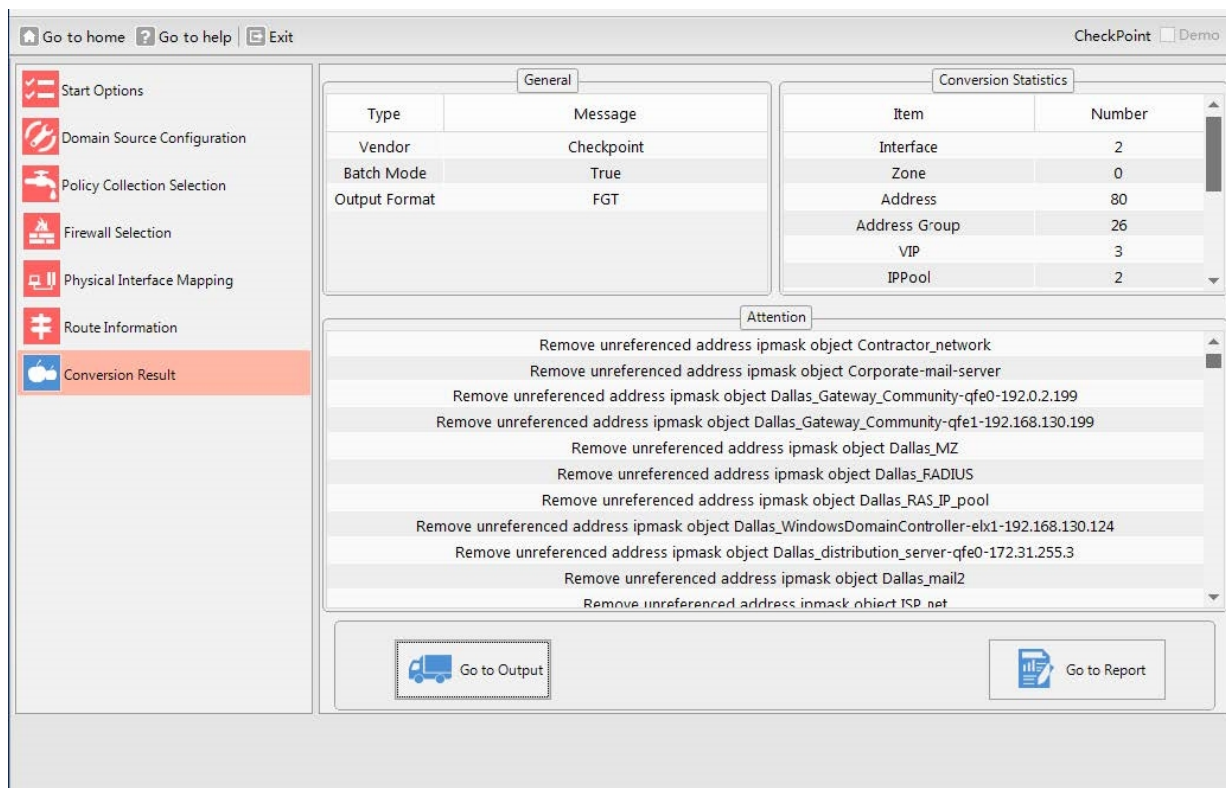
the Firewall Selection page (Check Point) or Device Selection page (Alcatel-Lucent), select **Retail Branch Batch Mode**.



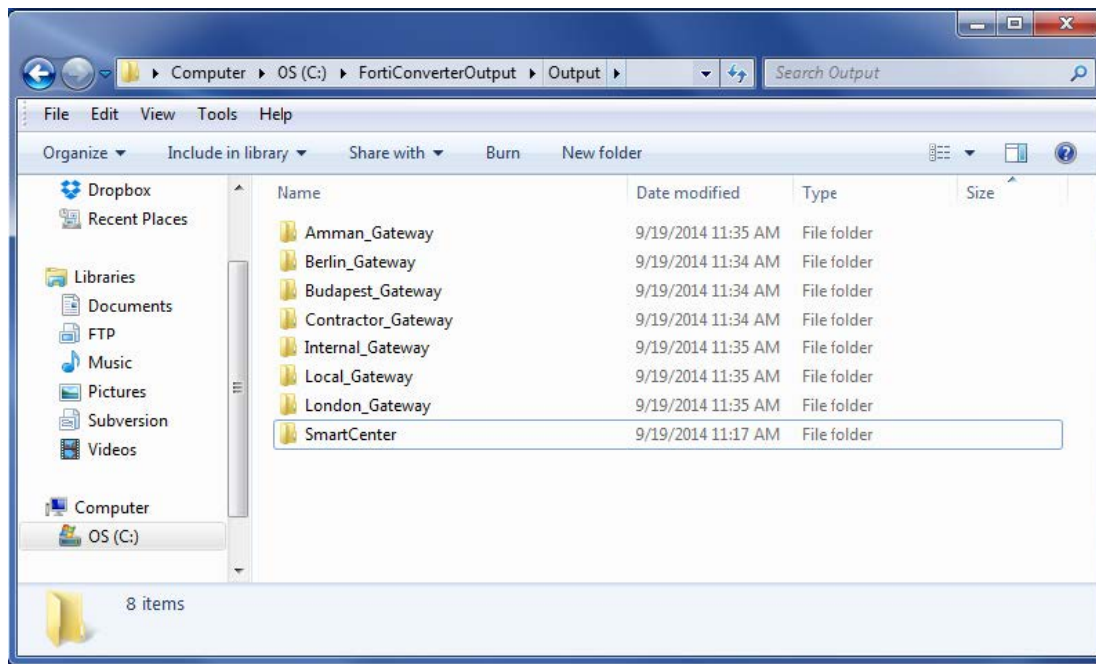
Select the firewalls to convert. Batch conversion requires that all the firewalls have the same number of network interfaces.



All other steps for using the wizard at the same as when you convert a single configuration, except for the **Conversion Result** page, which does not display the **Go to Tuning** option.



For batch conversions, the wizard saves each configuration file in its own directory in the output directory.



Viewing the results of your automatic conversion

The Conversion Result page displays general conversion information, statistics on of the number of converted objects and policies, and a log of items that need further attention.

To see a summary of the conversion, click **Go to Report**.

An HTML page generated by FortiConverter is displayed in your web browser.

Checkpoint Provider-1 to FortiManager

Domain: SmartCenter

Checkpoint Provider-1

- Firewall Objects
- Device List
- Unconverted
- Policy Packages
 - Standard
 - star_local
 - star_local_v3

Address

Name	Subnet/Range/FQDN
Amman_Gateway-gfe0-172.16.11.1	172.16.11.1/32
Amman_Gateway-gfe1-192.0.2.20	192.0.2.20/32
Amman_network	172.16.11.0/24
Berlin_Gateway-gfe0-10.100.102.254	10.100.102.254/32
Berlin_Gateway-gfe1-192.168.102.1	192.168.102.1/32
Berlin_IDS	192.168.102.49/32
Berlin_network	192.168.102.0/24
Budapest_Gateway-hme0-172.16.12.1	172.16.12.1/32
Budapest_Gateway-le0-192.168.12.1	192.168.12.1/32
Budapest_network	172.16.12.0/24
Chicago_network	192.168.130.0/24
Contractor_Gateway-gfe0-10.70.61.2	10.70.61.2/32
Contractor_Gateway-gfe1-192.168.10.54	192.168.10.54/32
Corporate-mail-server	172.16.2.2/32
Dallas_CVP	192.168.24.79/32
Dallas_DMZ	192.168.24.0/24
Dallas_Gateway_primary-hme0-192.0.2.253	192.0.2.253/32
Dallas_Gateway_primary-gfe1-192.168.130.253	192.168.130.253/32
Dallas_Gateway_primary-gfe2-10.10.111.253	10.10.111.253/32
Dallas_Gateway_primary-gfe3-192.168.24.253	192.168.24.253/32
Dallas_Gateway_primary-gfe4-10.255.255.253	10.255.255.253/32
Dallas_Gateway_secondary-hme0-192.0.2.254	192.0.2.254/32
Dallas_Gateway_secondary-gfe1-192.168.130.254	192.168.130.254/32
Dallas_Gateway_secondary-gfe2-10.10.111.254	10.10.111.254/32
Dallas_Gateway_secondary-gfe3-192.168.24.254	192.168.24.254/32
Dallas_Gateway_secondary-gfe4-10.255.255.254	10.255.255.254/32

config firewall address

```

edit "Amman_Gateway-gfe0-172.16.11.1"
set subnet 172.16.11.1 255.255.255.255
next
edit "Amman_Gateway-gfe1-192.0.2.20"
set subnet 192.0.2.20 255.255.255.255
next
edit "Amman_network"
set subnet 172.16.11.0 255.255.255.255
next
edit "Berlin_Gateway-gfe0-10.100.102.254"
set subnet 10.100.102.254 255.255.255.255
next
edit "Berlin_Gateway-gfe1-192.168.102.1"
set subnet 192.168.102.1 255.255.255.255
next
edit "Berlin_IDS"
set subnet 192.168.102.49 255.255.255.255
next
edit "Berlin_network"
set subnet 192.168.102.0 255.255.255.255
next
edit "Budapest_Gateway-hme0-172.16.12.1"
set subnet 172.16.12.1 255.255.255.255
next
edit "Budapest_Gateway-le0-192.168.12.1"
set subnet 192.168.12.1 255.255.255.255
next
edit "Budapest_network"
set subnet 172.16.12.0 255.255.255.255
next
edit "Chicago_network"

```

To examine the converted objects and policies in detail, click **Go to Tuning**. A window that allows you to tune the output is displayed.

Policy Tuning NAT Tuning Conversion Log

Go to home Go to help Exit Back Export Import UTM-1-Cluster-P Generate Report

Policy

Name	From	To	Source	Destination	Service	Action	SrcN...	IPPool
0 10000	any;	any;	gGateway1_of_Good-Ba...	all;	Authenticated;	accept	<input type="checkbox"/>	
1 10001	any;	any;	all;	all;	gUnWanted;	deny	<input type="checkbox"/>	
2 10002	any;	any;	Primary_Management; Bu...	All_Intranet_Gateways;	ident; NBT; boo...	deny	<input type="checkbox"/>	
3 10003	any;	any;	Primary_Management;	All_Intranet_Gateways;	ANY;	deny	<input type="checkbox"/>	
4 100000	any;	any;	Corporate-mail-server;	all;	ANY;	accept	<input checked="" type="checkbox"/>	
5 100001	any;	any;	all;	Corporate-mail-server;	ANY;	accept	<input type="checkbox"/>	
6 100015	any;	any;	Dallas_mail1;	all;	ANY;	accept	<input checked="" type="checkbox"/>	
7 100016	any;	any;	all;	Dallas_mail1;	ANY;	accept	<input type="checkbox"/>	
8 100030	any;	any;	Dallas_mail2;	all;	ANY;	accept	<input checked="" type="checkbox"/>	

Firewall Objects

Name	MemberList	PolicyRef.
0 Amman_Gateway	Amman_Gateway-gfe0-172.16.11.1; Amman_Gateway-gfe1-192.0.2.20;	10
1 Berlin_Gateway	Berlin_Gateway-gfe0-10.100.102.254; Berlin_Gateway-gfe1-192.168.102.1;	10
2 Budapest_Gateway	Budapest_Gateway-hme0-172.16.12.1; Budapest_Gateway-le0-192.168.12.1;	11
3 Contractor_Gateway	Contractor_Gateway-gfe0-10.70.61.2; Contractor_Gateway-gfe1-192.168.10.54;	7
4 Dallas_Gateway_primary	Dallas_Gateway_primary-hme0-192.0.2.253; Dallas_Gateway_primary-gfe1-192.168.130.253; Dallas...	9
5 Dallas_Gateway_secondary	Dallas_Gateway_secondary-hme0-192.0.2.254; Dallas_Gateway_secondary-gfe1-192.168.130.254; ...	10
6 Dallas_InternalWebServer	Dallas_InternalWebServer-eb0-192.168.130.123;	2
7 Dallas_Radius	Dallas_Radius-hme0-172.31.255.2;	2
8 HQ_Web_Servers	Dallas_Web_Server2; Dallas_Web_Server;	5
9 IDS_sensors	Berlin_IDS; Dallas_IDS; Dallas_IDS_admin; Dallas_IDS_RnD; London_IDS; Paris_IDS; Tokyo_IDS;	4
10 London_Gateway	London_Gateway-gfe0-192.168.103.254; London_Gateway-gfe1-10.100.103.254;	10
11 Madrid_Gateway	Madrid_Gateway-gfe0-192.168.110.1; Madrid_Gateway-gfe3-192.0.2.4;	9

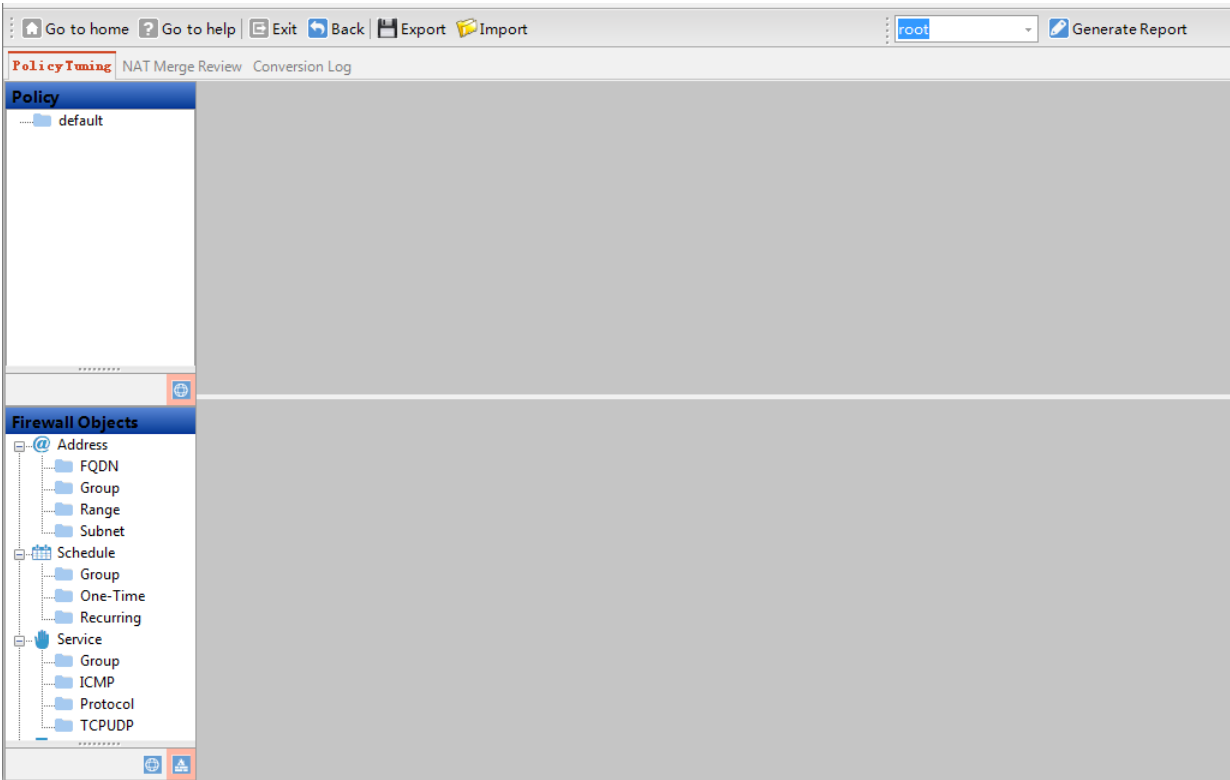
After your review and any tuning tasks are complete, click **Go to Output** to access the final, converted configuration files.

Tuning the FortiConverter output

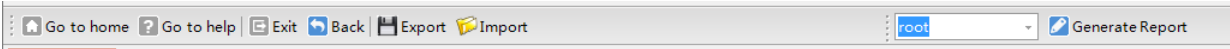
Although FortiConverter attempts to automatically convert as much of the source configuration as possible, in some cases, your input is required to complete the conversion. The Tuning page allows you to tune the results for your environment. To access the Tuning page, on the Conversion Result page, click **Go to Tuning**.



To quickly view a tuning "snapshot" (a configuration that you exported from the tuning page earlier), open the wizard for the appropriate vendor, click **Tuning** on any page, and then navigate to the snapshot file to import it.



Toolbar options



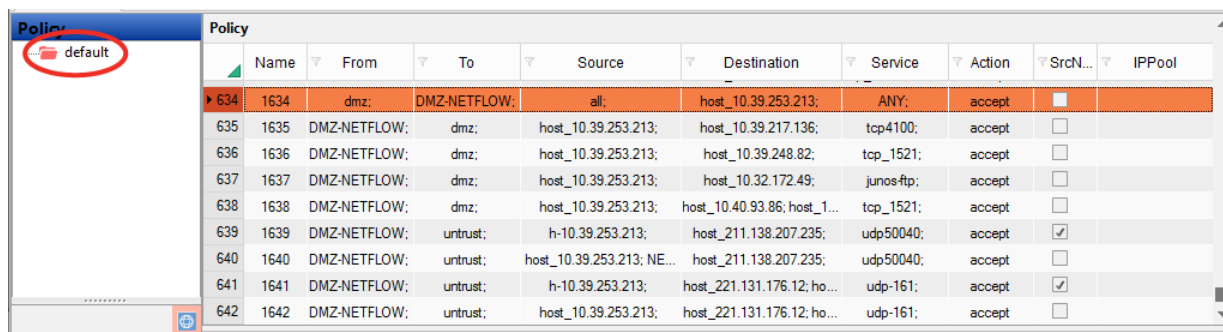
Item	Description
Go to home	Click to return to the main page.

Item	Description
Go to help	Click to open the latest version of this guide.
Exit	Click to close FortiConverter.
Back	Click to return to the Conversion Result page. FortiConverter preserves any changes but does not save them in an output file. (Use Generate Report to save changes to an output file.)
Export	Click to save the current configuration, including any modifications, to a text file (a tuning "snapshot").
Import	Click to import a configuration you exported earlier (a tuning "snapshot"). FortiConverter discards any changes in the current configuration.
VDOM	Select the VDOM in the output to display in the Tuning page.
Generate Report	Click to export the current configuration, including any modifications to an output configuration file .

Policy Tuning tab

The Policy Tuning tab allows you to review output policies and converted objects.

To review output policies, in the Policy navigation pane, select a package. The converted policies in the package are displayed.



	Name	From	To	Source	Destination	Service	Action	SrcN...	IPPool
634	1634	dmz;	DMZ-NETFLOW;	all;	host_10.39.253.213;	ANY;	accept	<input type="checkbox"/>	
635	1635	DMZ-NETFLOW;	dmz;	host_10.39.253.213;	host_10.39.217.136;	tcp4100;	accept	<input type="checkbox"/>	
636	1636	DMZ-NETFLOW;	dmz;	host_10.39.253.213;	host_10.39.248.82;	tcp_1521;	accept	<input type="checkbox"/>	
637	1637	DMZ-NETFLOW;	dmz;	host_10.39.253.213;	host_10.32.172.49;	junos-ftp;	accept	<input type="checkbox"/>	
638	1638	DMZ-NETFLOW;	dmz;	host_10.39.253.213;	host_10.40.93.86; host_1...	tcp_1521;	accept	<input type="checkbox"/>	
639	1639	DMZ-NETFLOW;	untrust;	h-10.39.253.213;	host_211.138.207.235;	udp50040;	accept	<input checked="" type="checkbox"/>	
640	1640	DMZ-NETFLOW;	untrust;	host_10.39.253.213; NE...	host_211.138.207.235;	udp50040;	accept	<input type="checkbox"/>	
641	1641	DMZ-NETFLOW;	untrust;	h-10.39.253.213;	host_221.131.176.12; ho...	udp-161;	accept	<input checked="" type="checkbox"/>	
642	1642	DMZ-NETFLOW;	untrust;	host_10.39.253.213;	host_221.131.176.12; ho...	udp-161;	accept	<input type="checkbox"/>	

To add a new policy to a package

1. Right-click a policy, and then click **New**.
2. Complete the settings, and then click **OK**.

To renumber the policies

1. Right-click the policy where you want the numbering to restart, and then click **ConfigPolicyIndex**.
2. For **Set Policy Index Start With**, enter the initial policy number to use, and then click **OK**.

635	1635	DMZ-NETFLOW;	dmz;	host_10.39.253.213;	host_10.39.217.136;	tcp4100;	accept	<input type="checkbox"/>	
▶ 636	1636	DMZ-NETFLOW;	dmz;	host_10.39.253.213;	host_10.39.248.82;	tcp_1521;	accept	<input type="checkbox"/>	
637	1637	DMZ-NETFLOW;	dmz;	host_10.39.253.213;	host_10.39.172.49;	junos-ftp;	accept	<input type="checkbox"/>	
638	1638	DMZ-NETFLOW;	dmz;	host_10.39.253.213;	host_10.39.248.82;	tcp_1521;	accept	<input type="checkbox"/>	

To edit the details for a converted policy

Double-click the policy and edit the settings as required.

Policy Edit Form ✕

Name

From

To

Source

Destination

Service

Schedule

Action **Log Allowed Traffic** **Status**

☐ Enable NAT

☒ Use Interface

☐ Use IPPool

Comments

Label

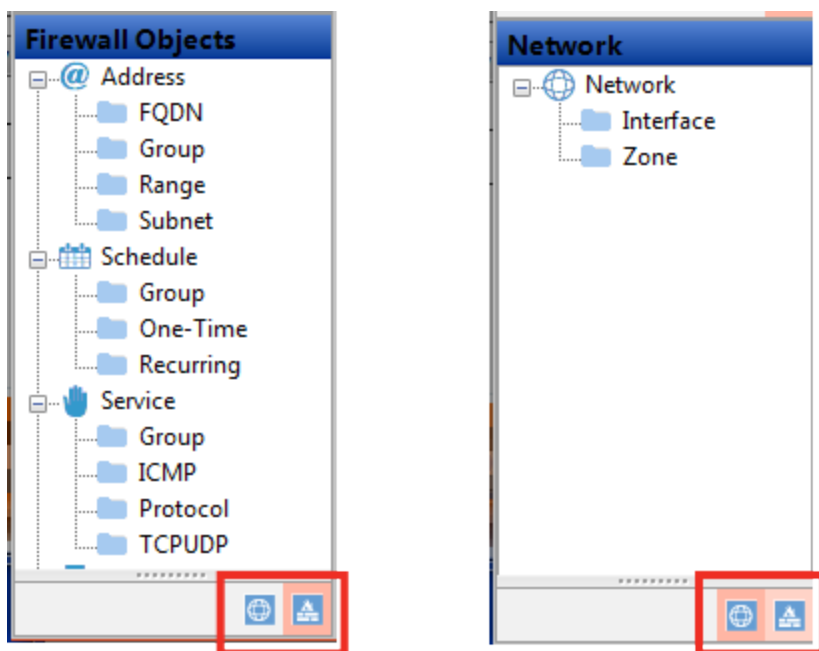
Item	Description
Name	You cannot edit this value.
From	Select source interface(s).

Item	Description
To	Select destination interface(s).
Source	Select source address object(s).
Destination	Select destination address object(s).
Service	Select service object(s).
Schedule	Select schedule object. – select to enable NAT, and then select to use Interface or IPPool Comments – modify the comments for the policy Label – modify the label of the policy
Action	Specify whether traffic is accepted or denied.
Log Allowed Traffic	Specify whether logging is enabled.
Status	Specify whether the policy is enabled.
Enable NAT	Select to enable NAT, and then do one of the following: <ul style="list-style-type: none"> • Select User Interface. • Select Use IPPool and specify a pool.
Comments	Edit the comments for the policy.
Label	Edit the label for the policy.

To review and edit firewall objects and interfaces

1. Go to the navigation pane at the bottom-left of the Policy Tuning tab.

Click the icons at the bottom of the pane to switch between firewall objects and interfaces.



- To view objects, select a category in the navigation pane.

Firewall Objects		Address Group		
		Name	MemberList	PolicyRef.
18	dongxin-wlan-mq-data-intra-group	dongxin-intra-10.39.248.85; dongxin-intra-10.39.248.88; dongxin-intra-10.39.248.26; wlan-test-server;...		1
19	extra-211.138.199.6-7-group	extra-net-199-6; extra-net-199-7;		2
20	extra-218-219-group	extra-net-218; extra-net-219;		1
21	ip-not-access-internet-group	ip-not-access-internet-12; ip-not-access-internet-13; ip-not-access-internet-14; ip-not-access-internet-...		1
22	lianchuangsyslog	lianchuangsyslog-1; lianchuangsyslog-2; lianchuangsyslog-3; lianchuangsyslog-4;		2
23	permit-ssh-telnet-rdp-group	DMZServer4A2; blzj;		1
24	phone-video	dongxin-intra-10.39.248.85; dongxin-intra-10.39.249.42; dongxin-intra-10.39.249.48;		1
25	td-ganzhipingtai-extra-group	td-ganzhipingtai-extra-1; td-ganzhipingtai-extra-2;		2
26	wlan-topology	dongxin-intra-10.39.248.26; wlan-test-server;		1
27	wlanac	SUZAC02BHW; XUZAC02BHW;		65
28	xinyewu-tiyan-intra-group	xintiyanzhongxin; xinyewu-tiyan-intra-net;		1
	Click to Enter a New Entry			0

- To add a new object, scroll to the bottom of the list, click in an empty row, and then complete the fields as required.

28	xinyewu-tiyan-intra-group	xintiyanzhongxin; xinyewu-tiyan-intra-net;	1
	Click to Enter a New Entry		0

- The PolicyRef column displays the number of policies that reference that firewall object.

Click the PolicyRef. column for the entry to display the specific policies in the Policy table above.

You cannot delete objects that are referenced by any other part of the configuration.

To filter rows to display only matching data

You can filter every column that has the [filter mark] by a given option or custom expression.

To delete a line of the configuration

Click the policy or object you want to delete to select it, and then press the Delete key.

You cannot delete items that are used by another policy or group.

To reorder rows

To reorder rows, click the policy number and drag the row to the new position.

NAT Merge Review tab

Currently, the NAT Merge Review tab allows you to review of the NAT policy conversion logic for Check Point and Juniper Junos OS conversions only.

Junos NAT Merge Review

You can use the sub-tabs in the top-right corner to select the NAT category to display: Source NAT, Destination NAT, Static NAT, Object NAT, Double NAT, and NAT Rule. The source configuration determines which categories are available.

Go to home Go to help Exit Back Export Import root Generate Report

Policy Tuning **NAT Merge Review** Conversion Log

Static NAT Source NAT **Destination NAT**

Destination NAT Rule Set *

Rule Name	From	Source	Destination	Service	IP Pool/Interface
96-101-2222240-248-10-22	dmz	-	211.139.96.101/32	-	pool-248-10-22

Security Rule

No.	Name	From	To	Source	Destination	Service	Action	Schedule	Status
0	bst_v5mq	untrust	dmz	any	host_10.39.249.42	TCP21000-21004	permit	always	Enabled
1	shujucaiji	untrust	dmz	host_221.181.240...	host_10.39.248.70	UDP3055	permit	always	Enabled
2	policy-051	untrust	dmz	dongxin-netflow-ex...	dongxin-netflow-int...	dongxin-netflow-sr...	permit	always	Enabled
3	tousu-ftp	untrust	dmz	net218.206.87.12...	dmz-248-73	tcp41400-41413	permit	always	Enabled
4	shoujizhongduan	untrust	dmz	any	host_10.40.103.230	tcp8888	permit	always	Enabled
5	dongxin-wlan-syslo...	untrust	dmz	dongxin-wlan-cha...	dongxin-intra-10.3...	tcp_514	permit	always	Enabled
6	PK-zhishiku	untrust	dmz	any	host_10.40.102.17	junos-http	permit	always	Enabled
7	BOSCH-manager	untrust	dmz	any	host_10.39.248.114	tcp_18081	permit	always	Enabled

To display a particular rule set from the source configuration, for **Destination NAT Rule Set**, select the appropriate value.

Destination NAT Rule Set *

The top pane of the NAT Merge Review tab is a list of NAT rules from the source configuration. Double-click a NAT rule to display the corresponding items in the Security Rule list (bottom pane).

Double-click a security rule to open the Merge Result window.

The screenshot shows the 'Merge Result' window with the following data:

NAT Rule Entry											
Type	Rule Set/Rule	From	To	Orig. Source	Orig. Dest	Orig. Service	Trans. Source	Trans. Dest	Trans. Service		
Source	source-nat-1/rule...	dmz	untrust	10.0.0.0/8	0.0.0.0/0	-	pool1-4	-	-		

Security Rule Entry										
No.	Name	From	To	Source	Destination	Service	Action	Schedule	Status	
129	v5v6booe	dmz	untrust	host_10.39.248.70; host_10.40.100.67	112.25.20.88	TCP8000-8003	permit	always	Enabled	

Fortigate Policy Entry									
Name	From	To	Source	Destination	Service	Action	SrcNAT	IP Pool	
100489	dmz	untrust	host_10.39.248.70; host_10.40.100.67	112.25.20.88	TCP8000-8003	accept	enabled	pool1-4	
10129	dmz	untrust	host_10.39.248.70; host_10.40.100.67	112.25.20.88	TCP8000-8003	accept	disabled	-	

Merge Summary

```

Comparing "from" field between Junos Source NAT rule and security rule...

Source NAT Rule :
  From zone [ dmz ]

Policy :
  From zone [ dmz ]

==> Result :
  Policy and Source NAT Rule "from" field overlapped

-----

Comparing "to" field between Junos Source NAT rule and security rule...

Source NAT Rule :
  To zone [ untrust ]

Policy :
  To zone [ untrust ]

==> Result :
  Policy and Source NAT Rule "to" field overlapped
  
```

The Merge Result window displays the NAT rule, the security rule, and the resulting FortiGate policies.

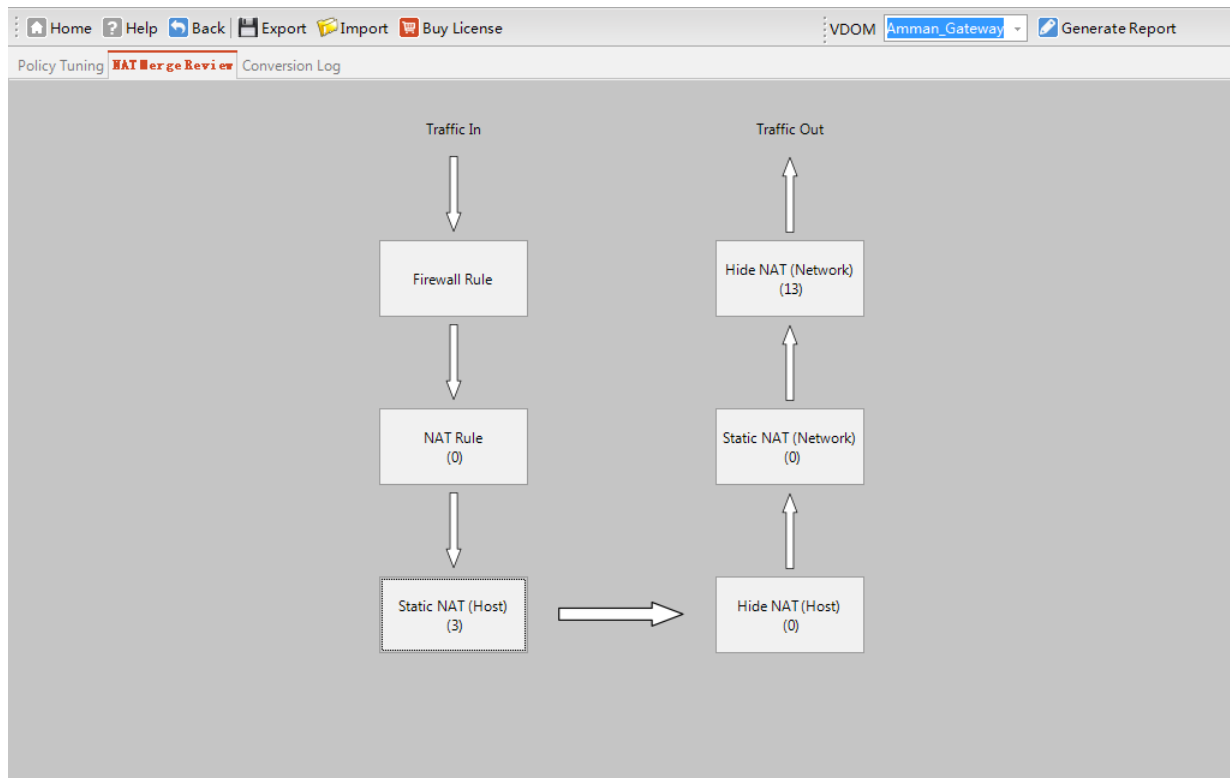
Policies that FortiConverter generated from a security rule from the source configuration have a five-digit name that is 10000 or higher.

Policies that FortiConverter generated by merging a NAT rule and security rule from the source configuration have a six-digit name that is 100000 or higher.

The Merge Summary provides a step-by-step description of the merge logic.

Check Point NAT Merge Review

For Check Point, the NAT merge review tab displays the different NAT types as tiles in a diagram.



Click a tile to access the NAT rules and merge logs for that NAT type.

NAT Merge Review

Hide Network Nat

Name	Real Address	Mapped Address
Amman_network	172.16.11.0/24	interface
Berlin_IP_Pool	10.199.3.254-10.199.3.254	interface
Berlin_network	192.168.102.0/24	10.100.102.254
Budapest_network	172.16.12.0/24	10.133.12.1
Dallas_IP_Pool	10.199.1.1-10.199.1.254	interface
Dallas_admin_network	172.31.255.0/24	interface
London_network	192.168.103.0/24	interface
Madrid_network	192.168.110.0/24	interface
NY_network	192.168.100.0/24	interface
Paris_IP_Pool	10.199.2.1-10.199.2.254	interface

Check Point Rule

View	Rule Base	Name	Source Address	Destination Add...	Service	Action	Schedule	Status	Firewall
View Merge	Standard	10000	gGateway1_of_G...	Any	Authenticated	accept	Any	Enabled	Any
View Merge	Standard	10001	Any	Any	gUnWanted	drop	Any	Enabled	Any
View Merge	Standard	10002	Primary_Manage...	All_Intranet_Gate...	ident; NBT; bootp	drop	Any	Enabled	Any
View Merge	Standard	10003	Primary_Manage...	All_Intranet_Gate...	Any	drop	Any	Enabled	Any
View Merge	Standard	10004	Any	Any	Any	accept	Any	Enabled	Any

Click a network name, and then click **View Merge** to display detailed information about the input and output rules.

Check Point Nat Merge To Check Point Rule Rule Summary

Input

Check Point Nat										
Type	Name	Real Address	Mapped Address							
Hide Network	Amman_network	172.16.11.0/24	interface							

Check Point Rule										
Rule Base	Name	Source Address	Destination Add...	Service	Action	Schedule	Status	Firewall	User	
star_local	10033	world_internal_ne...	Any	Allowed_policy_v2	"Client Auth"	Any	Enabled	Any	-	

Output

FortiGate Nat Policy From Merging Check Point Nat and Check Point Rule										
View	Name	From	To	Source	Destination	Service	Action	IPPool		
View Summary	100066	any	any	Amman_network	Amman_network	Allowed_policy_v.2	accept	-		
View Summary	100067	any	any	Amman_network	all	Allowed_policy_v.2	accept	source		

To view conversion log information about the merge, click **View Summary**.

NatMergeSummaryTextDialog										
Comparing "source address" field between Check Point Hide NAT rule and policy...										
Hide NAT Rule :										
Object Name [Amman_network]										
Policy :										
Source Address [world_internal_networks]										
==> Result :										
Policy "source address" and NAT Object field overlapped										
Detail address overlap information:										
NAT Object:										
[Amman_network]										
Expanding NAT Object...										
"Amman_network" is not expandable										
Policy Source Address:										
[world_internal_networks]										
Expanding Policy Address Book...										
"world_internal_networks" expand to [Amman_network;										
Berlin_network;										
Budapest_network;										
Chicago_network;										
Dallas_RnD_network;										
Dallas_admin_network;										
Dallas_network;										
London_network;										
Paris_network;										
Tokyo_network]										
								Copy Text	Close	

Conversion log tab

The Conversion Log tab displays warnings that FortiConverter generated during the conversion process.

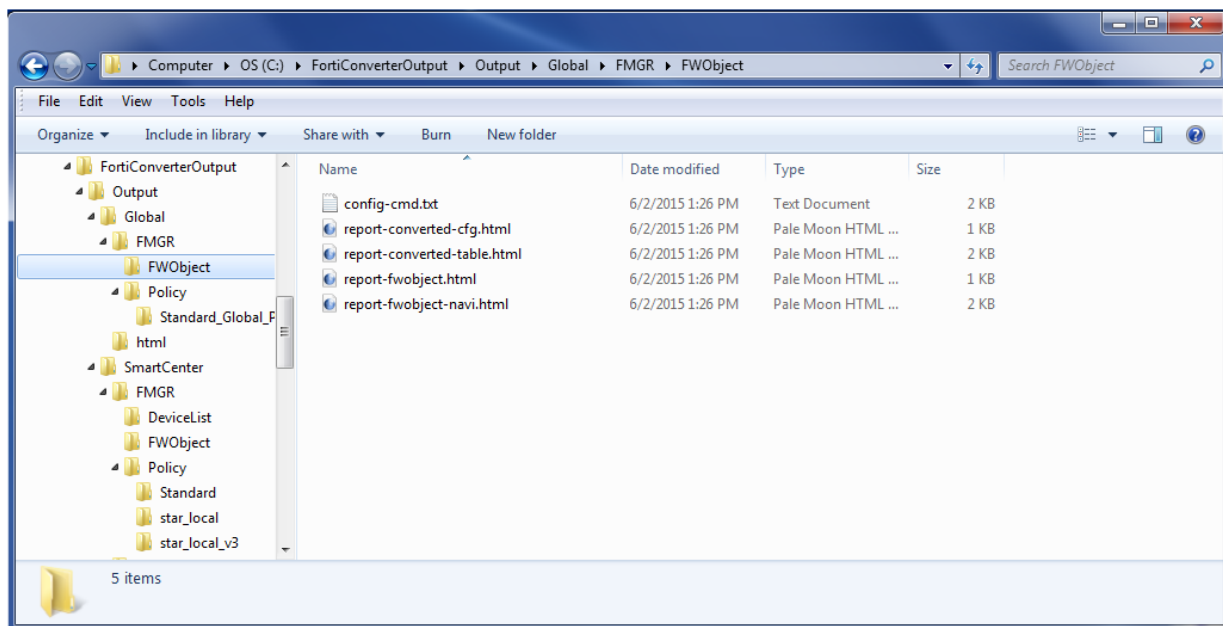
Policy Tuning NAT Merge Review Conversion Log				
	Level	Time	From	Content
0	Warning	2015-04-27 18:39:26.736	Common	Unsupported groups -> node0 -> system
1	Warning	2015-04-27 18:39:26.736	Common	Unsupported groups -> node0 -> snmp
2	Warning	2015-04-27 18:39:26.736	Common	Unsupported groups -> node1 -> system
3	Warning	2015-04-27 18:39:26.736	Common	Unsupported groups -> node1 -> snmp
4	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 10.39.130.170/32
5	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 10.39.248.29
6	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 10.39.249.173
7	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 211.103.0.110
8	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 211.103.0.110/32
9	Warning	6:39 PM	Address	Remove unreferenced address ipmask object 211.103.0.15
10	Warning	6:39 PM	Address	Remove unreferenced address ipmask object Agent
11	Warning	6:39 PM	Address	Remove unreferenced address ipmask object BV\$forDMZIP
12	Warning	6:39 PM	Address	Remove unreferenced address ipmask object CmnnetAgent
13	Warning	6:39 PM	Address	Remove unreferenced address ipmask object CmnnetDMZ-Ugate
14	Warning	6:39 PM	Address	Remove unreferenced address ipmask object CmnnetUgate
15	Warning	6:39 PM	Address	Remove unreferenced address ipmask object DMZtest211.103.0.87
16	Warning	6:39 PM	Address	Remove unreferenced address ipmask object IPNET
17	Warning	6:39 PM	Address	Remove unreferenced address ipmask object IPNET-REPORT
18	Warning	6:39 PM	Address	Remove unreferenced address ipmask object IPNETDX
19	Warning	6:39 PM	Address	Remove unreferenced address ipmask object IPnet_211.103.0.16
20	Warning	6:39 PM	Address	Remove unreferenced address ipmask object ISA
21	Warning	6:39 PM	Address	Remove unreferenced address ipmask object JTKH-REMOTE1
22	Warning	6:39 PM	Address	Remove unreferenced address ipmask object JTKH-REMOTE2
23	Warning	6:39 PM	Address	Remove unreferenced address ipmask object VMWARE-DMZ
24	Warning	6:39 PM	Address	Remove unreferenced address ipmask object VMWARE-WIN2003

Importing your new configuration into FortiManager

Output from conversion to FortiManager

After you convert a configuration to FortiManager, the output is organized in by source and type in multiple folders and text files.

For example, in the following illustration, the output files for a converted Checkpoint Provider-1 configuration are organized by source: Global and SmartCenter. They are further organized within each source by the following types: FWObject (network objects), Policy, and DeviceList (device configuration). The Policies folder contains a sub-folder for each source policy package.



Each FWObject and DeviceList folder and each Policy subfolder contains a config-cmd.txt. You use the contents of this text file to create FortiManager scripts that add the new configuration to your FortiManager instance.

To help you organized the import process and make troubleshooting easier, use a separate script for each config-cmd.txt. Alternatively, you can combine all the output files into a single script.

To avoid errors, run the scripts that you create using the contents of the FWObject folders first. If you use a single script, ensure that the commands from the FWObject folders come first in the script details. Policies that refer to an undefined object generate errors and interrupt the script.

Import your new configuration into FortiManager



Object scripts should be run before policy scripts. Policies that refer to an undefined object generate errors and interrupt the script.

1. In FortiManager, go to **System Settings > Admin > Admin Settings**.

Importing a converted configuration requires the scripting feature, which is hidden by default.

2. Select **Show Script**.

FortiManager-VM64

Device Manager Policy & Objects FortiGuard **System Settings**

System Settings

- Dashboard
- All ADOMs
- Network
- HA
- Admin
 - Administrator
 - Profile
 - Remote Auth Server
 - Admin Settings**
- Certificates
- Event Log
- Task Monitor
- Advanced

Settings

Administration Settings

HTTP Port: 80 ☒ Redirect to HTTPS

HTTPS Port: 443

HTTPS & Web Service Server Certificate: server.crt

Idle Timeout: 15 (1-480 Minutes)

Language: Auto Detect

☐ Password Policy

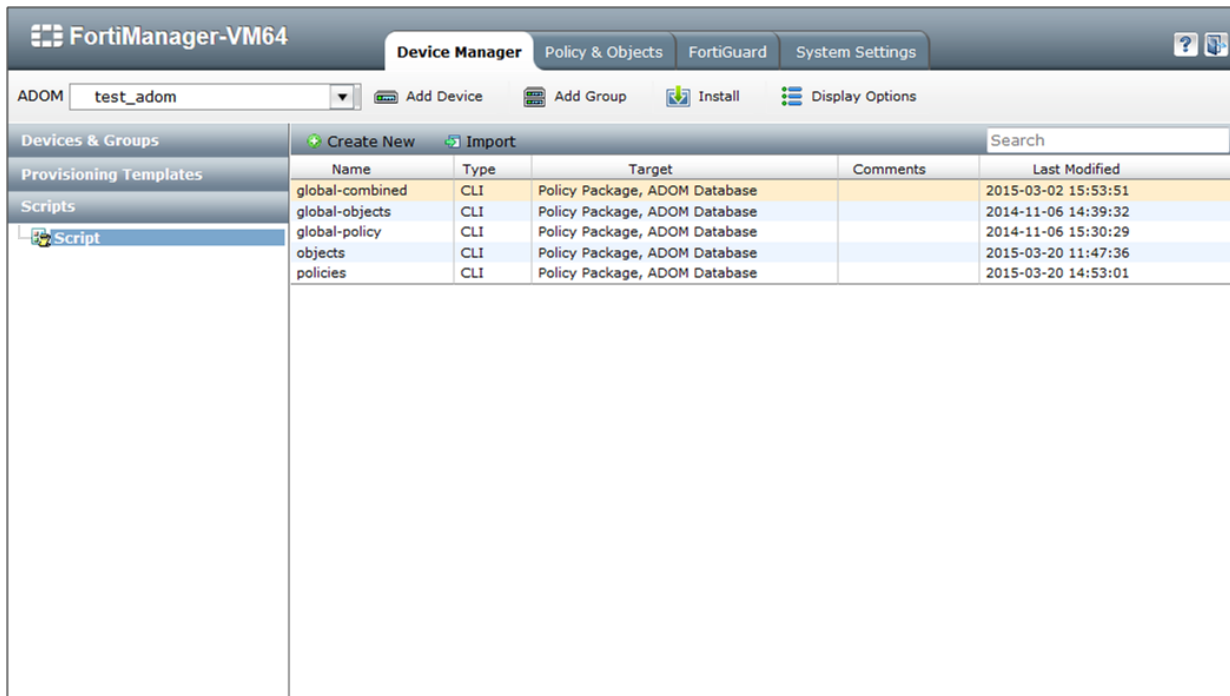
Display Options on GUI

☒ Show VPN Console ☒ Show Script

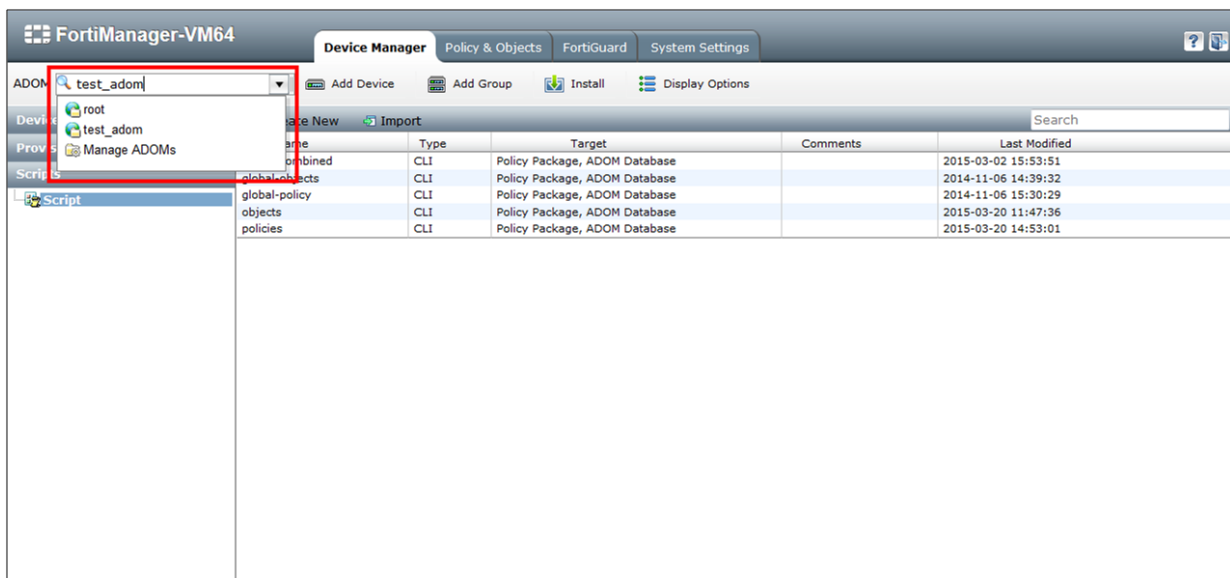
☐ Show Device List Import/Export ☐ Show Add Multiple Button

Apply

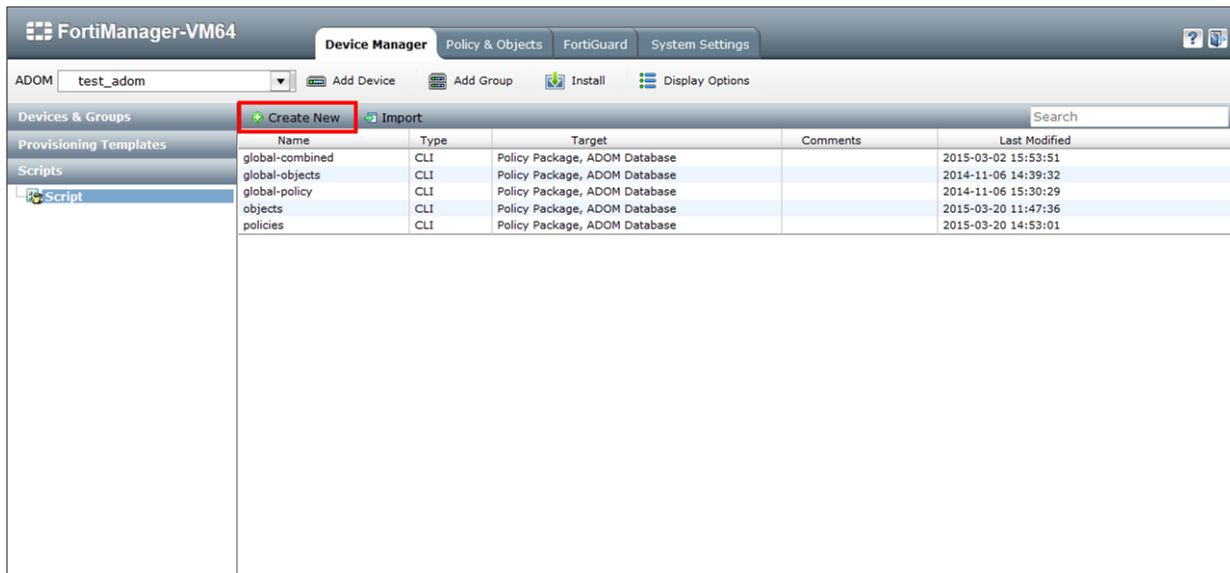
- On the **Device Manager** tab, go to **Scripts > Script**.



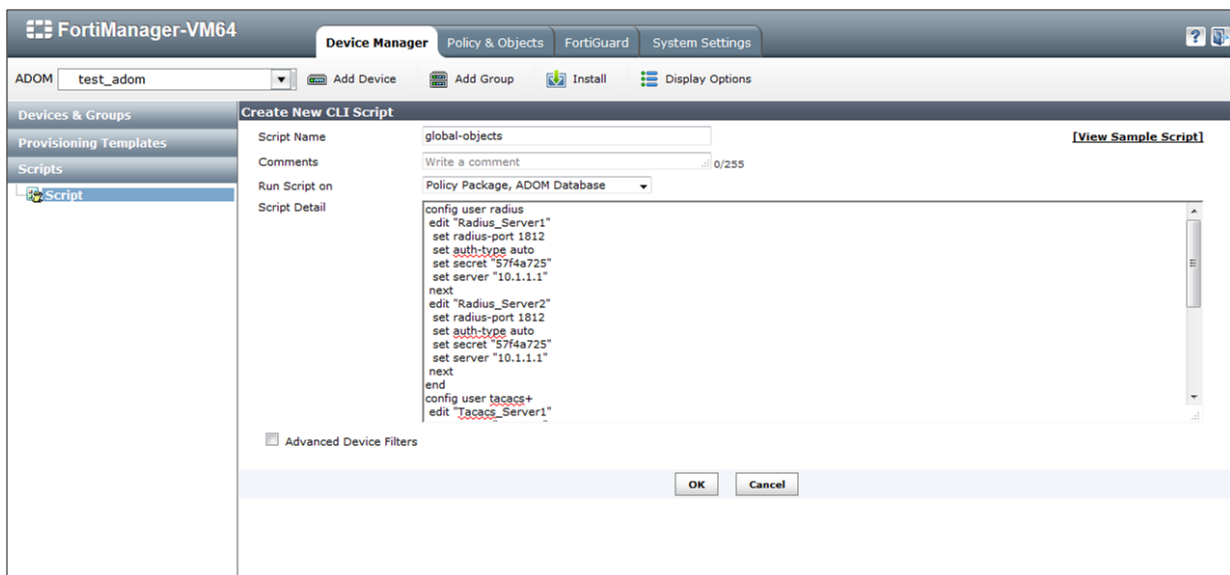
- For **ADOM**, select the ADOM that you want to import the configuration into.



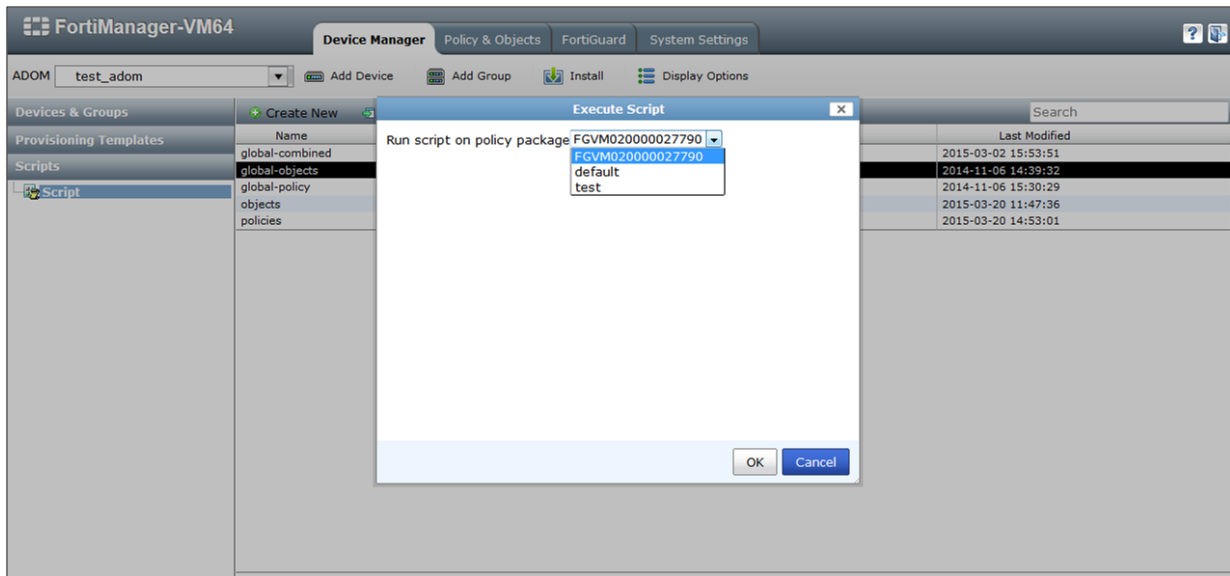
- To create a new script, click **Create New**.



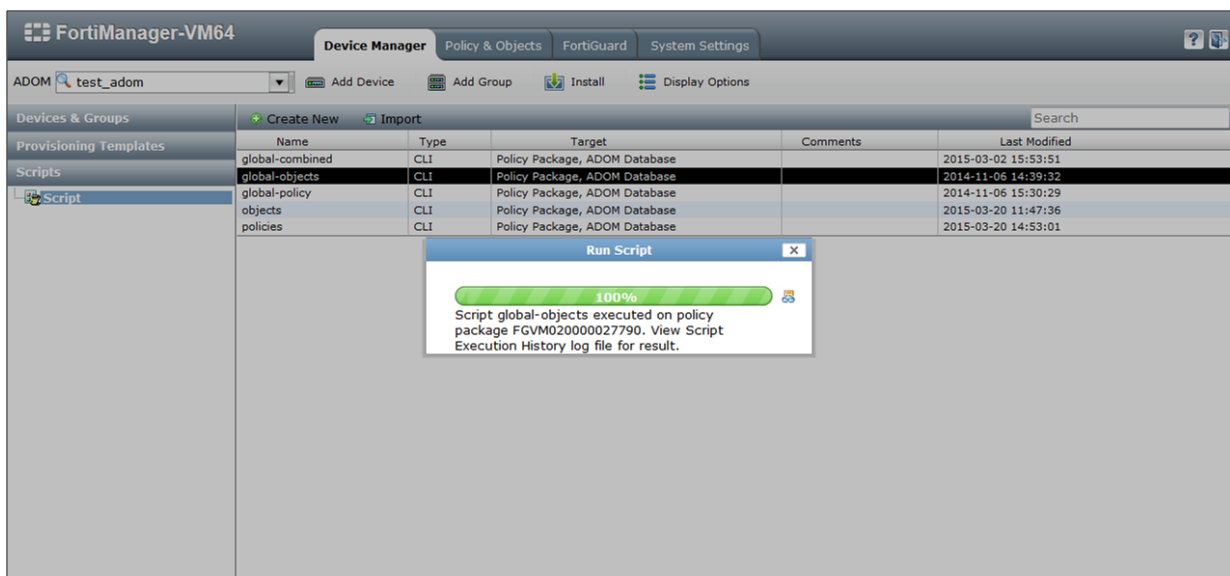
- Enter a name for the script and for **Run Script on**, select **Policy Package, ADOM Database**.
- For **Script Detail**, paste the content of one or more config-cmd.txt files.



- Click **OK** to save the script.
- In the list of scripts, right-click the script that you created, and then click **Run**.
- For **Run script on policy package**, select a target, and then click **OK**.



A progress bar is displayed.



11. If you are importing the configuration using multiple scripts, repeat the script creation and run process for the remaining config-cmd.txt files.

Understanding your new configuration

To help you understand your new configuration, review the differences between FortiGate and FortiManager and your previous firewall.

Alcatel-Lucent differences

Conversion support

FortiConverter supports the conversion of the following Alcatel-Lucent Brick features:

- Interfaces
- Host Groups
- Service Groups
- Zone Brick Rulesets

Fortinet plans to support for the following Lucent features in a future FortiConverter release:

- NAT
- Schedule
- VPN
- Hosts Behind Zone

Address and address group configuration

- Lucent host addresses are mapped to FortiGate addresses.
- Lucent host groups are mapped to FortiGate address groups.
- Virtual Brick Addresses (VBA) are not supported.

Interface configuration

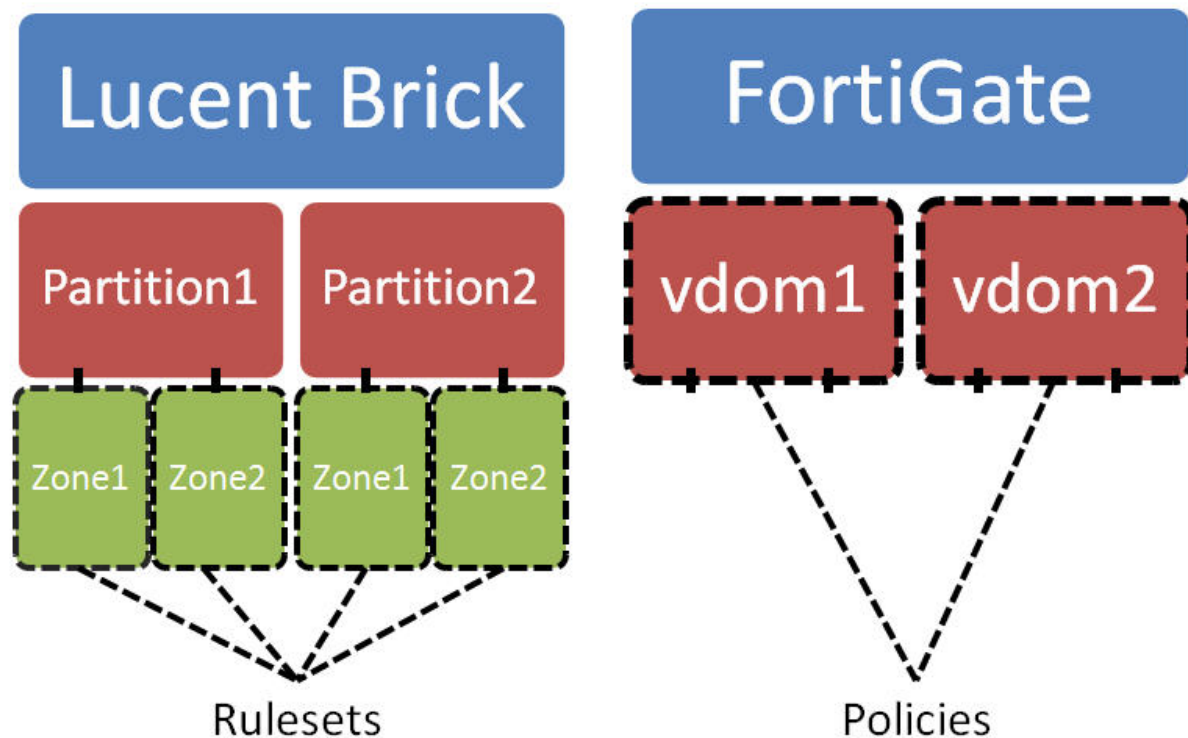
- FortiConverter assigns default VLAN configuration directly to physical interfaces.
- FortiConverter considers all VLANs named "*" or "Port Default" to be the default VLAN configuration.
- Domain Addresses are not supported.

Service and Service Group configuration

- Lucent Service Groups are mapped to FortiGate Service Groups.
- Lucent service "*" maps to FortiGate service "any".

Policy configuration

Lucent Brick Zone Rulesets operate at the zone level, which has no direct equivalent in FortiGate. Zone rulesets need to be translated into equivalent FortiGate policies.



FortiConverter translates Lucent Brick rules by separating traffic into two categories: inter- partition and intra- partition.

- **Inter-partition traffic** behaves like inter-VDOM traffic, and is simple to convert to FortiGate policies.
- **Intra-partition traffic** is more complicated to convert because multiple zone rules can be applied.

FortiConverter handles the inter-partition traffic by creating a general policy for each rule.

FortiConverter handles the intra-partition traffic by looking for all matches between two zone rulesets. FortiConverter looks at 3 fields: source, destination, and service. All 3 fields must overlap for the rules to match. FortiConverter creates a policy for each match using the intersection of each field.

The action of the rules determines the action of the converted policy, as shown in the following table:

Rule 1	Rule 2	Policy
Pass	Pass	Accept
Pass	Drop	Deny
Drop	Pass	Deny
Drop	Drop	Deny

Inter-partition Deny policies have higher priority than intra-partition policies, while inter- partition Accept policies have lower priority than intra-partition policies.

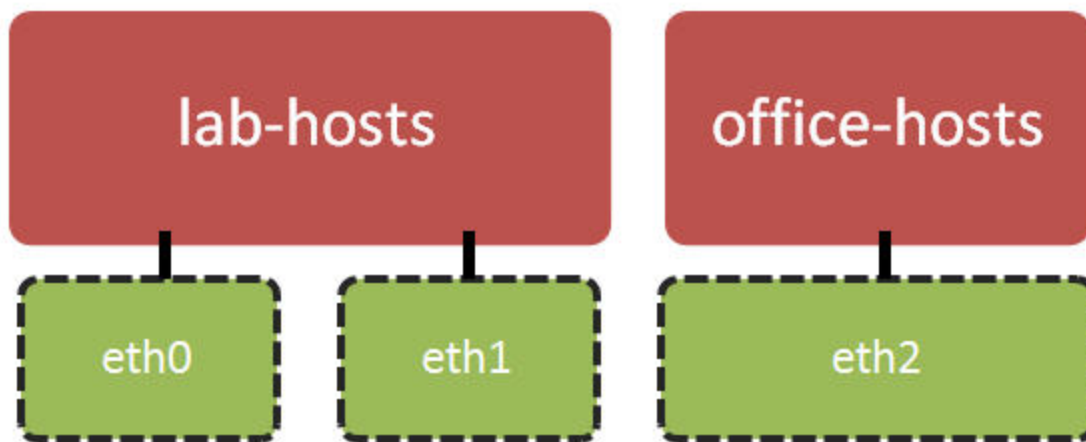
Lucent default rulesets “firewall” and “administrativezone” are currently unsupported.

VDOM configuration

- Lucent partitions map to FortiGate VDOMs.
- VDOM names are limited to 11 characters. FortiConverter truncates longer names to 11 characters.
- Lucent partition “*Default” maps to the FortiGate root VDOM.

Example conversion

The following block diagram and tables illustrates a Lucent configuration with 2 partitions and 3 zones.



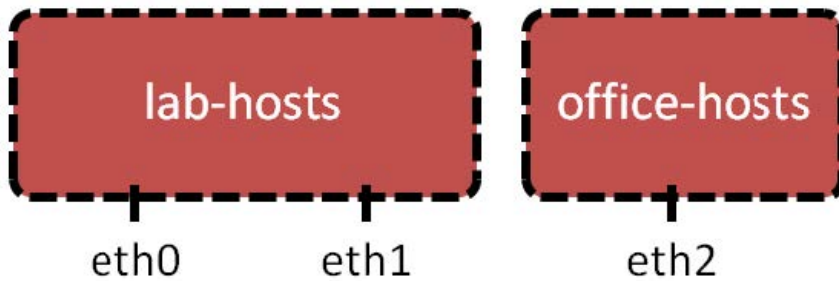
Zone eth0 Ruleset					
Rule Num	Direction	Source	Destination	Service	Action
1000	Out	192.168.1.15	172.30.10.1/24	*	Drop
1001	Both	192.168.1.0/24	172.30.10.1/24	*	Pass

Zone eth1 Ruleset					
Rule Num	Direction	Source	Destination	Service	Action
1000	In	*	172.30.10.5 - 172.30.10.20	TCP	Pass
1001	Both	192.168.1.132	172.30.10.9	*	Pass

Zone eth2 Ruleset

Rule Num	Direction	Source	Destination	Service	Action
1000	Both	*	10.10.15.0/24	HTTP	Pass

This Lucent configuration creates the following FortiGate configuration. Inter-partition rules are in **bold**.



VDOM lab-hosts Policies

Policy Num	Src Interface	Dst Interface	Source	Destination	Service	Action
10000	eth0	any	192.168.1.15	172.30.10.1/24	*	Deny
10001	eth0	eth1	192.168.1.0/24	172.30.10.5 - 172.30.10.20	TCP	Accept
10002	eth0	eth1	192.168.1.132	172.30.10.9	*	Accept
10003	eth0	any	192.168.1.0/24	172.30.10.1/24	*	Accept
10004	any	eth0	192.168.1.0/24	172.30.10.1/24	*	Accept
10005	eth1	eth0	192.168.1.132	172.30.10.9	*	Accept
10006	eth1	any	192.168.1.132	172.30.10.9	*	Accept
10007	any	eth1	192.168.1.132	172.30.10.9	*	Accept

VDOM office-hosts Policies

Policy Num	Src Interface	Dst Interface	Source	Destination	Service	Action
10000	any	eth2	any	10.10.15.0/24	HTTP	Accept
10001	eth2	any	10.10.15.0/24	any	TCP	Accept

Check Point differences

General

- FortiGate's `set allowaccess` command for interfaces does not exist on Check Point. Because FortiGate requires this setting, FortiConverter by default enables all services for interfaces.
- The interface "Lead to Internet" is a default static route on FortiGate.

Schedule configuration

FortiConverter converts "Day in month" time schedules to FortiGate one-time schedules. It converts "Day in week" and "None" schedules to recurring schedules.

You assign a year range for the "Day in month" schedule. If the specified day does not exist for a certain month, FortiConverter does not generate the one-time schedule for that month.

For example, the Check Point firewall's "Day in month" time schedule has the following parameters for each year:

```
Month: Jan/March/Sept.  
Day: 1, 5, 31  
Start and end time: 0:00 to 10:00
```

If you select `1` for **Convert 'Day in Month' to 'One Time Schedule' for next x years** in the FortiConverter conversion wizard and the current year value for the PC running FortiConverter is 2013, the wizard generates the following output for FortiGate one-time schedules:

```
From 0:00 Jan/1/2013 To 10:00 Jan/1/2013  
From 0:00 Jan/5/2013 To 10:00 Jan/5/2013  
From 0:00 Jan/31/2013 To 10:00 Jan/31/2013  
From 0:00 Match/1/2013 To 10:00 Match/1/2013  
From 0:00 Match/5/2013 To 10:00 Match/5/2013  
From 0:00 Match/31/2013 To 10:00 Match/31/2013  
From 0:00 Sept./1/2013 To 10:00 Sept./1/2013  
From 0:00 Sept./5/2013 To 10:00 Sept./5/2013
```

Notice that FortiConverter does not generate a Sept. 31 schedule.

NAT and policy configuration

- In Check Point, static NAT is a 1-to-1 IP relationship. In the FortiGate NAT policy found in the converted configuration, source NAT with an IP pool is not a 1-to-1 relationship.
- FortiConverter converts rule actions with "Client Auth" to FortiGate user-identity policies with the "Accept" action.
- FortiConverter does not convert NAT global properties.

VPN configuration

- Check Point does not configure VPN within a firewall rule. When FortiConverter converts the configuration to FortiGate, it generates several VPN policies from non-"Lead to Internet" interfaces to the "Lead to Internet" (default route) interface.
- After FortiConverter converts the VPN configuration, the VPN policy's destination interface refers to the "Lead to Internet" interface.

If you changed the default route's egress interface, you may need to update the VPN/Policy configuration manually.

Service objects

Unlike FortiGate service objects, Check Point service objects have a protocol type attribute. FortiGate uses a session helper object to provide the same functionality as the service objects with a protocol type attribute.

Cisco IOS, PIX or ASA differences

- FortiGate's `set allowaccess` command for interfaces does not exist on Cisco firewalls. Because FortiGate requires this setting, FortiConverter by default enables all services for interfaces.
- Cisco `object-group` objects have two types of service definitions. Because FortiGate services have both a source and destination port, FortiConverter can only convert `service-object` items into FortiGate services. By default, it does not convert the other type of service object, defined by `port-object`. FortiConverter generates FortiGate service objects from a Cisco ACL's protocol and source/destination port.
- On Cisco IPSec VPNs, Phase 1 (ISAKMP) supports more than two types of authentication methods. FortiGate supports only two types: `pre-share` and `rsa-sig`. Therefore, you must assign methods for each VPN connection. The wizard converts Cisco EZVPN configuration to FortiGate VPN policies from the "Intranet" interface to the interface which was assigned by the `crypto map interface` command.
- FortiConverter does not support the following Cisco configuration elements:
 - ASA objects for NAT and double NAT
 - Identity NAT and NAT Exemption
 - Wild card netmasks for `access-list` and `object-group` objects
 - EZVPN conversion

For example, FortiConverter does not support `crypto ipsec profile <profile-name>` and `crypto isakmp profile <profile-name>`.

- To reduce the number of NAT policies a conversion generates, FortiConverter does not convert Static NAT rules in which the source and mapped IPs are the same.

"FortiConverter supports Static NAT, Policy NAT, Dynamic NAT, and PAT. Identity NAT and NAT Exemption are not supported. Static NAT also supports identity translation - where the source and mapped are the same, these rules are not converted, reducing the number of NAT policies generated by the conversion.

Juniper ScreenOS or Junos OS differences

- FortiConverter recognizes interface names starting with "vlan" as logical interfaces.
- Junos service objects support MS-RPS and SUN-RPC, where program-numbers (SUN) and UUID (MS) are used instead of ports. FortiOS supports this configuration using Application Control with an application override.

Example of Junos service object conversion

```
config application list
edit "MS-ActiveDirectory"
config entries
edit 1
set application 152305667
config parameters
edit 1
set value "45f52c28-7f9f-101a-b52b-08002b2efabe"
next
edit 2
set value "811109bf-a4e1-11d1-ab54-00a0c91e9b45"
next
end
set action pass
next
end
next
end

edit 10012
set srcintf "trust"
set dstintf "mgn"
set srcaddr "MEI-Nov1-172.24.81.0-24" "MEI-Nov1-172.24.80.0-24" "MEI-Nov1-172.24.252.112-28"
set dstaddr "MEI-WAN"
set service "MS-ActiveDirectory"
set schedule "always"
set logtraffic all
set status enable
set action accept
set comments "95"
set application-list "MS-ActiveDirectory"
next
```

Palo Alto Networks OS (PAN-OS) differences

Conversion support

FortiConverter does not support the following features

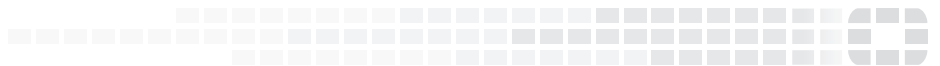
- VPN
- IPv6 address ranges
- IPv6 address subnets (will be supported in a future release)
- UTM

Configuration notes

- PAN-OS handles NAT and firewall policies with two separate modules, while FortiGate handles NAT within its policy module. FortiConverter makes a best effort attempt to map NAT rules onto each policy during the conversion, but you should review the results for accuracy.
- FortiConverter converts PAN-OS weekly schedules to FortiGate weekday schedules that are stored in a schedule group.



High Performance Network Security



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.